7 PHẠM TRÙ PHÒNG NGỪA TẤN CÔNG TỪ CHỐI DỊCH VỤ

Tấn công từ chối dịch vụ (DDoS) sẽ luôn là mối đe doạ hàng đầu đến các hệ thống trên thế giới. Về kỹ thuật, hầu như chúng ta chỉ có thể hy vọng attacker sử dụng nhựng công cụ và có hiểu biết kém cỏi về các protocol để có thể nhận biết và loại trừ c&

Tấn công từ chối dịch vụ (DDoS) sẽ luôn là mối đe doạ hàng đầu đến các hệ thống trên thế giới. Về kỹ thuật, hầu như chúng ta chỉ có thể hy vọng attacker sử dụng nhựng công cụ và có hiểu biết kém cỏi về các protocol để có thể nhận biết và loại trừ các traffic gây nên cuộc tấn công. Một điều mà các chuyên gia ai cũng thừa nhận, đó là nếu DDoS được thực hiện bởi một hacker có trình độ, thì việc chống đỡ là không thể. Cách đây 4 năm, giới hacker chính quy thế giới đã khai tử kỹ thuật tấn công này và chấm dứt mọi hoạt động nghiên cứu-trình diễn hay phát tán công cụ do chính bản thân họ cũng nhìn thấy mức độ nguy hiểm và không công bằng của kiểu tấn công này. Đối với hacker đẳng cấp thì "Hacking is get root!" Với một hạ tầng mạng hết sức yếu kém, cùng với nền thương mại điện tử vừa chớm hình thành, DDOS sẽ là một mối nguy hại rất lớn cho internet Việt Nam. Tất cả thành viên cộng đồng internet Việt Nam, nên có một cái nhìn và hành động thật chính chắn, DDOS là một hành động hết sức vô nghĩa về mọi mặt ! Tấn công từ chối dịch vụ (DoS) là các cuộc tấn công trên hệ thống mạng nhằm ngăn cản những truy xuất tới một dịch vụ. Tấn công DoS phá hủy dịch vụ mạng bằng cách làm tràn ngập số lượng kết nối, quá tải server hoặc chương trình chạy trên server, tiêu tốn tài nguyên của server, hoặc ngăn chặn người dùng hợp lệ truy nhập tới dịch vụ mạng. Có rất nhiều các phương cách để thực hiện các cuộc tấn công từ chối dịch vụ, vì thế cũng có rất nhiều cách phân loại DoS. Cách phân loại phổ biến thường dùng dựa vào giao thức trong hình thức tấn công của DoS, ví dụ như tràn ngập ICMP với Smurf, Ping of Death, khai thác điểm yếu của TCP trong hoạt động của giao thức và phân mảnh gói tin với SYN flood, LanD attacks, TearDrop hay trên mức dịch vụ như với Flash Crowds (ở Việt Nam thường biết đến với tên X-flash). Phân loại theo phương thức tấn công, DoS có thể được thực hiện bằng một vài gói tin đơn lẻ gửi thẳng tới server gây rối loạn hoạt động (như slammer worm), hoặc kích hoạt để gửi từ nhiều nguồn (từ chối dịch vụ phân tán – DdoS). Tấn công có thể thực hiện trên mạng Internet (sử dụng ngay các web server), hoặc broadcast trong mạng bên trong (insider attacks – như với Blaster worm), trên mạng P2P (P2P index poinsioning) hay Wireless (WLAN authentication rejection attack-spoof sender). Tuy nhiên, có thể thấy các cách phân loại trên dựa chủ yếu vào cách nhìn từ sự phát sinh tấn công, và vì thế, không hệ thống hóa được phương thức phòng tránh. Một cách chung nhất, có 7 phạm trù các tổ chức cần xem xét khi đối phó với các mối đe dọa về DoS như sau: 1/ Phòng ngừa các điểm yếu của ứng dụng (Application Vulnerabilities) Các điểm yếu trong tầng ứng dụng có thể bị khai thác gây lỗi tràn bộ đệm dẫn đến dịch vụ bị chấm đứt. Lỗi chủ yếu được tìm thấy trên các ứng dụng mạng nội bộ của Windows, trên các chương trình webserver, DNS, hay SQL database. Cập nhật bản vá (patching) là một trong những yêu cầu quan trọng cho việc phòng ngừa. Trong thời gian chưa thể cập nhật toàn bộ mạng, hệ thống phải được bảo vệ bằng bản vá ảo (virtual patch). Ngoài ra, hệ thống cần đặc biệt xem xét những yêu cầu trao đổi nội dung giữa client và server, nhằm tránh cho server chịu tấn công qua các thành phần gián tiếp (ví dụ SQL injection) 2/ Phòng ngừa việc tuyển mộ zombie Zombie là các đối tượng được lợi dụng trở thành thành phần phát sinh tấn công. Một số trường hợp điển hình như thông qua rootkit (Sony hay Symantec), hay các thành phần hoạt động đính kèm trong mail, hoặc trang web, ví dụ như sử dụng các file jpeg khai thác lỗi của phần mềm xử lý ảnh, các đoạn mã đính kèm theo file flash, hoặc trojan cài đặt theo phishing, hay thông qua việc lây lan worm (Netsky, MyDoom, Sophos).

Để phòng chống, hệ thống mạng cần có những công cụ theo dõi và lọc bỏ nội dung (content filtering) nhằm ngăn ngừa việc tuyển mộ zombie của hacker. 3/ Ngăn ngừa kênh phát động tấn công sử dụng công cụ Có rất nhiều các công cụ tự động tấn công DoS, chủ yếu là tấn công phân tán DDoS như TFN, TFN2000 (Tribe Flood Network) tấn công dựa trên nguyên lý Smurf, UDP, SYN, hay ICMP; Trinoo cho UDP flood; Stacheldraht cho TCP ACK, TCP NULL, HAVOC, DNS flood, hoặc tràn ngập TCP với packets headers ngẫu nhiên. Các công cụ này có đặc điểm cần phải có các kênh phát động để zombie thực hiện tấn công tới một đích cụ thể. Hệ thống cần phải có sự giám sát và ngăn ngừa các kênh phát động đó. 4/ Ngăn chặn tấn công trên băng thông Khi một cuộc tấn công DdoS được phát động, nó thường được phát hiện dựa trên sự thay đổi đáng kể trong thành phần của lưu lượng hệ thống mạng. Ví dụ một hệ thống mạng điển hình có thể có 80% TCP và 20% UDP và ICMP. Thống kê này nếu có thay đổi rõ rệt có thể là dấu hiệu của một cuộc tấn công. Slammer worm sẽ làm tăng lưu lượng UDP, trong khi Welchi worm sẽ tạo ra ICMP flood. Việc phân tán lưu lượng gây ra bởi các worm đó gây tác hại lên router, firewall, hoặc cơ sở hạ tầng mạng. Hệ thống cần có những công cụ giám sát và điều phối băng thông nhằm giảm thiểu tác hại của tấn công dạng này. 5/ Ngăn chặn tấn công qua SYN SYN flood là một trong những tấn công cổ nhất còn tồn tại được đến hiện tại, dù tác hại của nó không giảm. Điểm căn bản để phòng ngừa việc tấn công này là khả năng kiểm soát được số lượng yêu cầu SYN-ACK tới hệ thống mạng. 6/ Phát hiện và ngăn chặn tấn công tới hạn số kết nối Bản thân các server có một số lượng tới hạn đáp ứng các kết nối tới nó. Ngay bản thân firewall (đặc biệt với các firewall có tính năng stateful inspection), các kết nối luôn được gắn liền với bảng trạng thái có giới hạn dung lượng. Đa phần các cuộc tấn công đều sinh số lượng kết nối ảo thông qua việc giả mạo. Để phòng ngừa tấn công dạng này, hệ thống cần phân tích và chống được spoofing. Giới hạn số lượng kết nối từ một nguồn cụ thể tới server (quota). 7/ Phát hiện và ngăn chặn tấn công tới hạn tốc độ thiết lập kết nối Một trong những điểm các server thường bị lợi dụng là khả năng các bộ đệm giới hạn giành cho tốc độ thiết lập kết nối, dẫn đến quá tải khi phải chịu sự thay đổi đột ngột về số lượng sinh kết nối. Ở đây việc áp dụng bộ lọc để giới hạn số lượng kết nối trung bình rất quan trọng. Một bộ lọc sẽ xác định ngưỡng tốc độ kết nối cho từng đối tượng mạng. Thông thường, việc này được bằng số lượng kết nối trong thời gian nhất định để cho phép sự dao động trong lưu lượng. Các phân tích ở trên được dựa trên những ngầm định cơ bản sau trong việc bảo vệ hệ thống. Thứ nhất, đó là các thiết bị bảo vệ cần được đặt trên luồng thông tin và thực hiện trực tiếp việc ngăn ngừa. Điều này xuất phát từ lý do cho tốc độ của một cuộc tấn công (ví dụ khoảng 10.000 đăng ký thành viên trên 1s hướng tới 1 server, hoặc phát tán worm với tốc độ 200ms trên hệ thống mạng Ethernet 100M). Với tốc độ như vậy, cách thức phòng ngừa dạng phát hiện – thông báo ngăn chặn (Host Shun và TCP Reset) không còn phù hợp. Thứ hai, các cuộc tấn công từ chối dịch vụ chủ yếu nhắm tới khả năng xử lý của hệ thống mạng mà đầu tiên là các thiết bị an ninh thông tin. Năng lực xử lý của IPS hoặc các thành phần content filtering là một trong những điểm cần chú ý, đặc biệt ở sự ổn định trong việc xử lý đồng thời các loại lưu lượng hỗn tạp với kích thước gói tin thay đổi. Thứ ba, các cuộc tấn công luôn được tích hợp (blend attacks) với sự tổng hợp các phương thức khác nhau. Chính vì vậy, tầm quan trọng của việc phòng ngừa những dấu hiệu lây nhiễm đơn giản là bước đầu tiên để ngăn chặn những cuộc tấn công từ chối dịch vụ. Trong hệ thống tổng thể về security, để đối phó với các cuộc tấn công từ chối dịch vụ, thì thành phần IPS được coi là quan trọng nhất ở tính trong suốt với người dùng, nên việc phân tích các luồng thông tin trao đổi giữa server và người dùng không bị ảnh hưởng bởi các luồng tấn công hướng thẳng đến nó. Dưới đây là tóm tắt những báo cáo của NSS, tổ chức kiểm tra định khả năng các thiết bị

mạng trong môi trường giả lập tấn công cho các thiết bị IPS của các hãng hàng đầu - TopLayer Attack Mitigator IPS Theo đúng tên gọi, thiết bị này thực hiện việc chuyển dịch tấn công, không hẳn thực thi ngăn ngừa tấn công. Chính vì thế nên latency tăng cao trong môi trường bị tấn công. Toplayer được khuyến nghị khi sử dụng với đúng mục đích là thiết bị chuyển dịch tấn công. - ISS Proventia G ISS Proventia G cho thấy khả năng đáp ứng với hầu hết các loại tấn công với latency thấp, ngoại trừ DoS với packet nhỏ. ISS Proventia có thể được dùng trong hệ thống mạng nội bộ với hạ tầng không phải Gigabit. - McAffee IntruShield MacAffee IntruShield là một thiết bị được đánh giá có khả năng đáp ứng được yêu cầu về bao quát đầy đủ về dấu hiệu tấn công cũng như mức độ latency thấp. - TippingPoint UnityOne Đây là thiết bị duy nhất NSS cung cấp chứng chỉ NSS Gold (so với các chứng chỉ khác là NSS Approve). Ngoài việc đáp ứng tiêu chí latency và khả năng phát hiện các cuộc tấn công, UnityOne nhỉnh hơn McAffee IntruShield về khả năng dự báo phản hồi (predictable response) với mọi cuộc tấn công.