

CƠ CHẾ MỚI PHÒNG CHỐNG TẤN CÔNG DDOS GÂY BỞI THƯ RÁC

KS. Âu Xuân Phong

Tổ NCPT An toàn thông tin.

Tóm tắt: Các dịch vụ email của công ty thường được thiết kế để thực hiện tốt hơn so với các dịch vụ email công cộng. Một số thuận lợi nổi bật như là việc chuyển email nhanh, dung lượng file truyền đi lớn, khả năng bảo vệ chống spam và virus cao, môi trường quảng cáo thương mại miễn phí, nhưng các dịch vụ mail này thường xuyên là mục tiêu của các hacker hay spammer. Ngày nay việc tấn công DDoS thông qua việc spam ngày càng gia tăng, làm xáo trộn các dịch vụ mail của các tổ chức. Trong bài báo này giới thiệu một giải pháp mới để phòng chống tấn công DDoS gây bởi spam email, đó là việc kết hợp các bộ lọc nguồn đầu vào được tinh chỉnh, bộ lọc nội dung cùng chính sách triển khai email, đào tạo người dùng, giám sát mạng và các giải pháp hợp lý đối với các cuộc tấn công đang diễn ra. Theo thực tế, cơ chế phòng chống này đã giúp giảm tới 60% lưu lượng spam mail tới và đẩy lùi được nhiều cuộc tấn công DDoS gây bởi spam email.

1. GIỚI THIỆU

Email là công cụ được hàng triệu người sử dụng trong giao tiếp trên toàn thế giới. Tuy nhiên, spam đã gây trở ngại tới các email của người dùng, làm tiêu tốn tài nguyên, thời gian và tiền bạc của họ. Số lượng spam email chiếm tới 80% tổng lượng mail. Rất nhiều nhà nghiên cứu đã đưa ra nhiều giải pháp nhằm ngăn chặn việc spam. Tuy nhiên điều ấy cũng chỉ như một hạt nước được thả vào biển, các spammer luôn luôn tìm ra cách mới để có thể tiến hành thành công việc chuyển các spam email tới hộp thư của người dùng. Bên cạnh đó, một mục tiêu khác là các mail server, nhằm làm xáo trộn các hoạt động của công ty, làm mất đi tiền bạc cũng như danh tiếng của họ. DDoS là kiểu tấn công phổ biến làm tê liệt các hệ thống server. Bài báo này sẽ mô tả cơ chế tấn công DDoS thông qua việc spam mail và cơ chế phòng chống sử dụng cấu trúc đa lớp.

Chu kỳ sống của email: Các thư được soạn ở trong máy nguồn sẽ được chuyển giao tới MTA – Message Transfer Agent. MTA sẽ tìm máy đích nhờ sự giúp đỡ của DNS server và chuyển tiếp mail tới MTA của máy đích. MTA ở máy đích chuyển mail tới hộp thư của người dùng cuối. Các MTA chuyển tiếp mail với nhau sử dụng SMTP - Simple Mail Transfer Protocol.

Hầu hết các hệ thống mail công ty đều nhanh hơn và phức tạp hơn các hệ thống mail

miễn phí khác. Hệ thống mail công ty chuyên mail nhanh hơn và hỗ trợ chuyển file có dung lượng lớn cũng như có không gian lưu trữ không giới hạn. Để chuyển thư nhanh hơn, các server bỏ qua hầu hết các bước kiểm tra spam. Để đính kèm được file dung lượng lớn, nó phải bỏ qua các thiết lập chọn lọc nội dung. Điều ấy khiến cho các mail server công ty có nhiều lỗ hổng để tấn công spam mail, gây ra các cuộc tấn công DDoS.

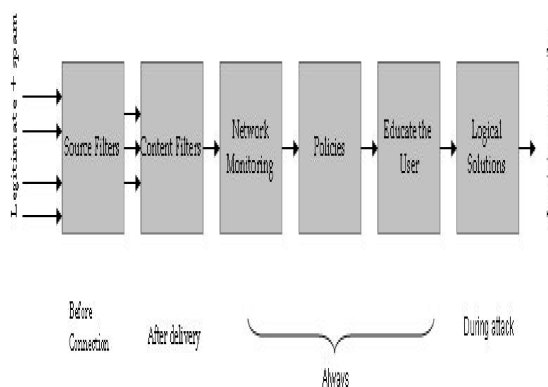
Phần dưới của bài báo được sắp xếp như sau: Mục 2 cung cấp kiến thức nền tảng về cơ chế tấn công DDoS thông qua spam và các ảnh hưởng của nó. Mục 3 miêu tả cơ chế phòng chống kiểu tấn công này. Mục 4 trình bày một số kết quả thử nghiệm. Tổng kết là mục 5.

2. CƠ CHẾ TẤN CÔNG DDOS THÔNG QUAN SPAM

Tấn công DDoS là kiểu tấn công trên quy mô rộng lớn tới các dịch vụ tại hệ thống của nạn nhân hay các nguồn tài nguyên mạng. Tấn công DDoS thông qua spam mail là một dạng của tấn công DDoS. Ở dạng này, attacker thâm nhập vào mạng bằng một chương trình được đính kèm vào spam mail. Sau khi khởi chạy file đính kèm đó, nguồn tài nguyên của mail server sẽ bị cạn kiệt dần bởi một số lượng lớn mail từ các máy khác trong domain gửi đến gây ra hiện tượng từ chối dịch vụ DoS. Attacker đã tạo ra các spam

mail vượt qua được bộ lọc spam và chuyển spam mail ấy tới hộp thư của người dùng.

Spam mail có đính kèm file .exe dung lượng nhỏ (ví dụ như update.exe). Attacker thường sử dụng file có 2 đuôi mở rộng để gây nhầm lẫn cho bộ lọc và người dùng (ví dụ như Update_KB2546_*86.BAK.exe). Các file đính kèm này thường có dung lượng nhỏ 140K đến 180K. Hầu hết các spam mail sẽ yêu cầu người nhận thực thi file .exe để update phần mềm anti-virus. Khi thực thi file, nó sẽ đưa file mới vào trong thư mục windows, thay đổi file registry, dẫn tới website của attacker để download các chương trình lớn nhằm gây hại cho mạng sau này. Các máy bị nhiễm độc sẽ thu thập các địa chỉ mail thông qua danh sách địa chỉ và tự động gửi mail tới các thành viên khác trong cùng domain. Thậm chí nếu người dùng không sử dụng các chương trình dịch vụ mail như Outlook express hay các phần mềm khác, nó sẽ tự gửi mail bằng cách sử dụng SMTP của chính nó. Hầu hết các spam mail sẽ tấn công vào các id của nhóm mail và sẽ gửi mail tới các nhóm ấy. Bằng cách này, nó sẽ phát tán nhanh và mạnh hơn rất nhiều. Nếu bất cứ người dùng nào chuyển tiếp mail này, thì tình hình sẽ còn tồi tệ hơn rất nhiều. Và cuối cùng server sẽ nhận được một số lượng lớn các yêu cầu từ các nơi, làm vượt qua khả năng xử lý của server, trở thành một cuộc tấn công DDoS. Loại sâu thường được dùng trong tấn công DDoS là WORM_start.Bt, WORM_STRAT.BG, WORM_STRAT.BR, TROJ_PDROPPER.Q. Khi được thực thi, các sâu này sẽ đưa các file serv.exe, serv.dll, serv.s, serv.wax, E1.dll, rasaw32t.dll ... vào thư mục của windows.



Hình 1. Cơ chế phòng chống đa lớp

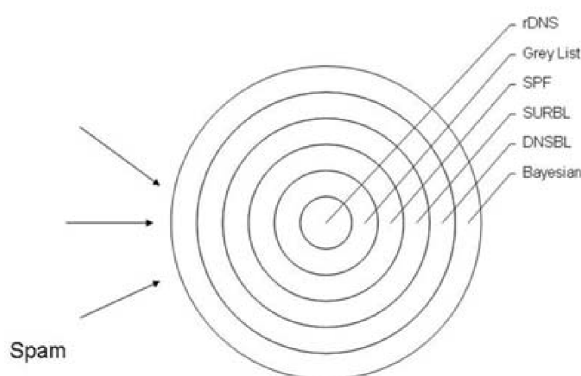
3. CƠ CHẾ PHÒNG CHỐNG

Bài báo đưa ra cơ chế sử dụng cấu trúc đa lớp để phòng chống tấn công DDoS gây bởi spam mail (hình 1).

Đó là sự kết hợp giữa việc các bộ lọc nguồn đầu vào được tinh chỉnh, bộ lọc nội dung, chính sách giám sát mạng, chính sách cho email, đào tạo người dùng và các giải pháp hợp lý, đúng lúc của người quản trị mạng. Sự kết hợp của các lớp này sẽ cung cấp phương thức tốt nhất để ngăn chặn tấn công DDoS thông qua spam mail.

3.1 Bộ lọc nguồn đầu vào

Hiện tại có rất nhiều bộ lọc nguồn đầu vào, tuy nhiên việc sử dụng tất cả các bộ lọc này sẽ không giúp cho việc ngăn chặn được hoàn toàn các cuộc tấn công mà còn làm cho quá trình chuyển mail bị chậm lại. Vì vậy việc tinh chỉnh bộ lọc là điều cần thiết. Hình 2 chỉ ra cấu trúc của bộ lọc nguồn đầu vào:



Hình 2. Sự kết hợp giữa các bộ lọc nguồn đầu vào.

Bộ lọc Bayesian: là bộ lọc có tính hiệu quả cao được sử dụng cho nhiều hệ thống anti-spam. Bộ lọc này hoạt động dựa trên các định lý toán học của nhà toán học Bayes. Trong phương pháp của Bayes, hệ thống sẽ xây dựng hai bảng từ các nội dung của spam mail gửi đến và các mail hợp lệ. Bảng này giống như một cuốn từ điển, mỗi từ trong mail mới gửi đến sẽ được so sánh với bảng spam mail và bảng mail hợp lệ ấy. Với các từ trong mail đến, các giá trị xác suất được tính toán dựa trên số lần xuất hiện của từng từ trong bảng spam mail và bảng mail hợp lệ. Ví dụ, từ “Viagra” xuất hiện 400 lần trong 3000

spam mail và 5 lần trong 300 mail hợp lệ, có xác suất là 0.889 $[400/3000]/[5/300+400/3000]$. Nó sẽ thực hiện quá trình này với tất cả các từ xuất hiện trong mail gửi đến. Các mail bị coi là spam nếu xác suất tính toán được cao hơn mức ngưỡng là 0.5. Ngưỡng thông thường là 0.7 và cao hơn đối với mail server công ty. Dựa đến mức độ đe dọa, người quản trị có thể thay đổi giá trị ngưỡng này. Sau khi phân loại các mail là spam, nội dung của spam sẽ được thêm vào trong từ điển. Nó sẽ rất hữu ích cho các tính toán sau này. Bằng cách này, hệ thống có thể học được các công nghệ mới nhất mà các spammer sử dụng. Người quản trị có thể bật hoặc tắt việc học này. Từ điển này thông thường chứa khoảng 50000 từ đối với các server nhỏ và vừa. Nếu như tăng kích thước của từ điển, thời gian tìm kiếm và thời gian xử lý sẽ tăng lên làm chậm quá trình chuyển mail. Hệ thống sẽ mất khoảng hai tuần để xây dựng bảng danh sách các từ spam, bên cạnh đó có một số bộ lọc sử dụng bảng danh sách tĩnh sẵn có. Các spammer đã học được cách để vượt qua bộ lọc này mặc cho quá trình học của bộ lọc diễn ra là liên tục. “Mail, server, report, firewall, virus, windows, customer, support” là một vài từ khóa thông dụng trong bảng mail hợp lệ và cũng được attacker sử dụng để tạo mail mẫu. Server sẽ gửi báo cáo với tiêu đề “server report” tới người quản trị mạng. Vì vậy xác suất để hệ thống nhận ra email này là spam sẽ là rất thấp. Bộ lọc Bayesian là rất tốt tuy nhiên nó không thể lọc được 100% các tin spam.

DNSBL: 80% các spam mail là đến từ các người dùng cá nhân. Nếu ta có danh sách các địa chỉ IP tạo spam, ta có thể chặn được các bản tin spam. DNSBL dựa trên nguyên tắc ấy. Danh sách DNS đen (DNSBL) là bộ lọc đầu vào rất tốt, nó hoạt động trước khi thực hiện quá trình chuyển mail tới hộp thư người dùng. Rất nhiều DNSBL đưa ra danh sách địa chỉ IP dựa trên nguồn open relay, spam hay virus. Các DNSBL được sử dụng rộng rãi nhất là spamhaus, spamcop, sorbs, abuseat, dsbl, rfc-ignorant ... đưa ra hàng nghìn địa chỉ IP của các nơi khởi tạo spam. Có thể có sự trùng lặp các IP trong các danh sách DNS đen này. Các mail hợp lệ chuyển đi sẽ bị chậm lại nếu tất cả danh sách DNS đen được sử dụng. Hầu hết các server đều có tùy

chọn bao gồm chọn nhiều hoặc xóa danh sách DNSBL bất kỳ. Tuy nhiên vẫn còn tới 20% các địa chỉ spam mail không được liệt kê trong DNSBL nên ta vẫn cần sử dụng thêm các bộ lọc khác hay phương thức khác để ngăn chặn spam.

SURBL: là một danh sách các spam website, domain, web server. Nếu có bất cứ URL hay địa chỉ IP nào trong bản tin, hệ thống sẽ kết nối với danh sách SURBL để kiểm tra xem URL đó có được liệt kê không. Nếu URL ấy được liệt kê trong SURBL, nó sẽ chặn bản tin đó lại. Danh sách SURBL hiện tại là sc.surbl.org, ws.surbl.org, ob.surbl.org, ab.surbl.org. Multi.surbl.org là kết hợp của tất cả các danh sách ấy. Tuy nhiên, nếu hệ thống sử dụng các SURBL khác với multi.surbl.org, nó sẽ mất thời gian khá lâu để xử lý mail. Nếu chỉ sử dụng duy nhất multi.surbl.org cho việc kiểm tra SURBL, và nếu dịch vụ không khả dụng, sẽ không có bước kiểm tra nào được thực hiện. Khuyến nghị ở đây là sử dụng 4 SURBL hơn là dùng multi.surbl.org. Việc dùng bộ lọc URL này rất có hiệu quả trong việc chống lại tấn công DDoS khi mà nó thường tham chiếu tới các website giả mạo. Một số attacker sử dụng nhiều URL nhằm gây nhầm lẫn cho bộ lọc. Việc kết hợp kiểm tra SURBL với các bộ lọc khác là cách tốt nhất để phòng chống tấn công DDoS.

Sender Policy Framework: Khung chính sách cho người gửi sẽ loại bỏ bản tin nếu việc kiểm tra SPF thất bại. Việc giả mạo địa chỉ người gửi là mối đe dọa lớn tới người dùng trong mạng. Id mail của attacker là giả, tuy nhiên lại có tên miền của nạn nhân, nên hầu hết người dùng nhận được mail đều tuân theo các chỉ dẫn và thực thi các file đính kèm, dẫn đến bị tấn công DDoS. Ta có thể chặn lại tấn công này bằng cách sử dụng SPF (Sender Policy Framework). SPF cho phép kiểm tra email của người gửi có phải giả mạo hay không trong bất cứ trường hợp nào. Ngày nay, hầu hết các spammer sử dụng email giả mạo nhằm che dấu danh tính của mình. SPF yêu cầu tổ chức của người gửi phải công khai mail server của họ vào trong bản ghi SPF. Nếu bạn nhận mail từ một người dùng, bạn có thể kiểm tra mail ấy có tới từ tổ chức hay không bằng địa chỉ IP của người gửi. Bản ghi SPF sẽ thông báo cho phía nhận rằng người

dùng ấy có được phép sử dụng mạng của họ hay không. Nếu tổ chức nhận ra đó là máy cá nhân, nó sẽ vượt qua bước kiểm tra này, ngược lại đó là attacker hay spammer.

Grey Listing: Grey Listing từ chối tất cả các mail tới từ các địa chỉ IP không quen thuộc với các mã lỗi. Mail server sẽ ghi lại tổ hợp các thông tin id và địa chỉ IP của cả người gửi và người nhận. Nếu người gửi ấy cố gắng gửi tiếp mail sau khoảng thời gian 10 giây đến 12 giờ, server sẽ kiểm tra tổ hợp trong bản ghi của mình, nếu trùng, nó sẽ cho phép người gửi chuyển tin nhắn. Điều này dựa trên thực tế rằng các spammer sẽ không cố gắng gửi lại thư trong khi người dùng hợp lệ thường sẽ làm như vậy. Tuy các spammer đã tìm ra cách để vượt qua, nhưng phương pháp này cũng đã giảm thiểu được lượng spam đáng kể.

Reverse DNS: Hệ thống nhận tin cần có rDNS. Hệ thống gửi tin cần có tên miền và địa chỉ IP để chứng tỏ nó được gửi đi từ người dùng hợp lệ. Hầu hết các spam đều không có reverse DNS. Việc từ chối tất cả các mail đến mà không có rDNS là một cách hiệu quả để lọc tin spam. “Từ chối bản tin nếu IP server gửi đi không có rDNS”, “Từ chối bản tin nếu đầu vào reverse DNS không khớp với Hello host” là 2 lựa chọn được cung cấp cho hầu hết các dịch vụ mail. SPF và rDNS rất hữu ích để lọc spam trong nhiều trường hợp mở rộng.

3.2 Bộ lọc nội dung

Bằng cách kiểm tra cẩn thận từng từ trong tiêu đề và nội dung mail, ta có thể chặn được spam. Hầu hết tiêu đề các tin spam đều cố gắng gây nhầm lẫn cho các bộ lọc. Spammer sẽ sử dụng các từ dễ nhận biết như 1 chủ đề và từ địa chỉ rõ ràng. Nếu các mail tới có nội dung hay chủ đề cá biệt, bộ lọc nội dung sẽ dừng ngay việc chuyển mail. Hầu hết các spam mail gây ra tấn công DDoS đều có chủ đề như test, server report, status, hello ... nhằm tránh bộ lọc nội dung. Ví dụ, “Server report” là từ được server dùng để gửi báo cáo tới người quản trị, nên các mail gửi đi có chủ đề này sẽ được coi là hợp lệ. Bộ lọc nội dung sẽ chặn các mail có vài từ cá biệt như Viagra, ViAgRa, install updates, customer support service ...

Trong DDoS, các cuộc tấn công sẽ đến từ bản thân các id của chính domain mail nên việc chặn mail id của chính nó là điều không khả thi. Một lựa chọn khác là ta có thể chặn tất cả các mail không gửi bởi người dùng cụ thể. Người quản trị có thể chặn tất cả các mail đến từ một nguồn nào đó hoặc các mail có dung lượng xác định, ví dụ như có thể chặn tất cả các mail đến có file đính kèm nặng quá 100 KB. Bộ lọc nội dung có thể chặn các mail với các định dạng file cụ thể (ví dụ như .exe), nhờ đó có thể chặn được DDoS. Tuy nhiên hiện nay attacker đã tìm cách vượt qua bằng cách sử dụng 2 đuôi mở rộng như update.doc.exe, update.txt.exe ... Nó sẽ gây nhầm lẫn cho bộ lọc và mail sẽ được chuyển tới hộp thư. Để tránh điều này, bộ lọc nội dung cung cấp thêm lựa chọn như lọc các định dạng *.*.exe. Điều này giúp ích rất nhiều cho việc phòng chống DDoS thông qua spam.

3.3 Chính sách

Mail là cách truyền thông chính giữa tất cả các nhân viên trong một tổ chức. Vì vậy cần có một quy ước cho email để phân biệt thông tin là Gửi hay Nhận. Một tổ chức dù lớn hay nhỏ đều cần một hệ thống thống nhất việc gửi, phân loại và sử dụng các tập tin trong mail server của họ. Người dùng được yêu cầu sử dụng các dấu hiệu nhận biết hoặc có thể đặt dấu hiệu nhận biết cho tất cả id trong một domain. Vì vậy người dùng có thể dễ dàng phân biệt các mail là spam hay hợp lệ. Hầu như mail của attacker sẽ không bao gồm bất cứ dấu hiệu nhận biết nào. Ví dụ như với các tổ chức tôn giáo, họ sẽ yêu cầu người dùng sử dụng các từ cụ thể để xác định mail đó là đến từ người dùng hợp lệ (người dùng dùng từ “In His Service” thay vì “regards” ở cuối mail). Attacker không thể xác định các từ cụ thể ấy. Các từ khóa sẽ giúp tách các spam mail ra khỏi mail hợp lệ. Người dùng sẽ không mở mail hay thực thi các file đính kèm, điều này giúp mạng chống lại tấn công DDoS thông qua spam một cách có hiệu quả.

3.4 Đào tạo người dùng

Hành động của người dùng trước và trong quá trình cuộc tấn công diễn ra đóng vai trò quan trọng trong việc phòng chống tấn công DDoS. Vì vậy người dùng cần được đào tạo cách xử lý với các trường hợp như vậy.

Họ phải được đào tạo về spam mail và tấn công DDoS.

- Yêu cầu người dùng không trả lời hay chuyển tiếp hay làm gì điều gì tương tự đối với các mail từ người dùng lạ.
- Yêu cầu thông báo cho người quản trị, nếu họ trả lời đó là spam thì người dùng nên đánh dấu flag spam để server chặn lại.
- Yêu cầu không dùng email dùng trong công việc để đăng kí các nhóm mới hay cho các mục đích khác.
- Yêu cầu không chạy bất cứ file exe nào được gửi tới mail.
- Tự động xóa các spam mail sau mỗi ngày làm việc.
- Sau cuộc tấn công DDoS, spam mail có thể xuất hiện trở lại và gây ra tấn công DDoS, vì vậy người dùng nên xóa mail cũ và spam mail của họ thường xuyên.

3.5 Giám sát mạng

Để phòng chống tấn công DDoS thông qua spam, cần thiết phải giám sát lưu lượng mạng theo thời gian thực. Các hành vi bất thường có thể được tìm thấy nếu mạng được giám sát 24/7. Nếu tốc độ của dịch vụ mail bị giảm, ta có thể cho rằng server đang phải xử lý một khối dữ liệu rất lớn. Thậm chí nếu lưu lượng mạng bị tắc nghẽn nặng, người quản trị có thể điều tiết được lưu lượng dữ liệu để tăng tốc độ mail. Tuy nhiên, trong cuộc tấn công, người quản trị mạng không thể điều tiết được dữ liệu như bình thường, họ có thể đánh giá đang có gì đó sai đang diễn ra trong mạng và đưa ra các biện pháp phòng chống. Giả sử có 2 mail server đang được giám sát với số lượng người dùng mail tối thiểu là 200. Nếu 1 domain bị tấn công DDoS thông qua spam, người quản trị có thể biết được và ngăn chặn không cho lây lan tới các mail server khác. Theo dõi lịch sử hoạt động của mạng và các vấn đề về mạng sẽ hữu ích để giải quyết các tình huống tức thời.

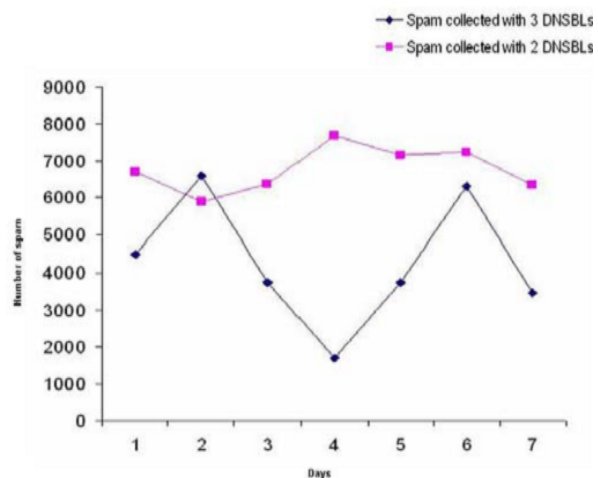
3.6 Giải pháp hợp lý.

Tùy theo kỹ năng của người quản trị, bất cứ cuộc tấn công nào cũng có thể được giải quyết mà ít gây ảnh hưởng đến hệ thống nhất. Sau cuộc tấn công, việc tắt server không thực sự hữu dụng, mà nên thay đổi đường dẫn của data dumping. Tấn công DDoS thông qua

spam thường nhắm tới mục tiêu là các nhóm id. Người quản trị có thể thay đổi toàn bộ nhóm id sang nhóm id mới (ví dụ như thay `allstaff@ABC.com` thành `all_staff@ABC.com`). Nhờ đó các spam mail sẽ đi chệch hướng và bị dừng ngay lập tức. Các máy bị tiêm nhiễm cần được tách rời khỏi mạng ngay và cần được phân tích để xem ảnh hưởng của cuộc tấn công. Sau khi loại bỏ các sâu độc hại, các máy ấy có thể tham gia vào mạng trở lại. Đó là giải pháp hợp lý cho các cuộc tấn công.

4. KẾT QUẢ THỬ NGHIỆM

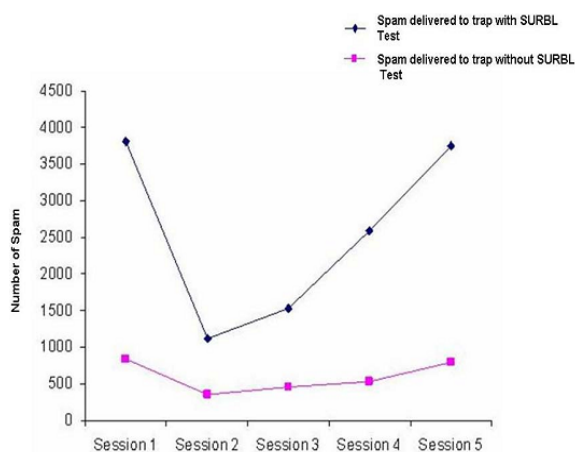
Hệ thống áp dụng thử nghiệm là hệ thống web server cung cấp dịch vụ cho 200 user với 20 nhóm email IDs và 200 mail riêng biệt. Tốc độ kết nối internet là 100 Mbps trong mạng LAN, tốc độ download và upload là 20 Mbps. Các spam mail sẽ được thu thập tại spam trap dựa theo cơ chế phòng chống đa lớp đề cập ở trên.



Hình 3. Hiệu quả khi áp dụng DNSBL

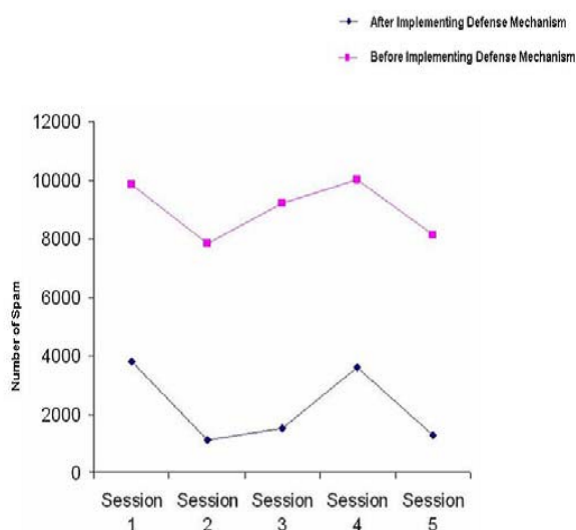
Kết quả thử nghiệm hiệu quả của DNSBL trong 2 trường hợp: sử dụng 3 trang `Relays.ordb.org`, `bl.spamcop.net`, `sbl.spamhaus.org` và sử dụng 2 trang `bl.spamcop.net`, `sbl.spamhaus.org`. Ta thấy, khi không có trang `Relays.ordb.org` trong DNSBL, lưu lượng spam đã tăng lên 40-50%

Kết quả thử nghiệm hiệu quả của SURBL. Ta tiến hành theo dõi việc chuyển mail vào các thời điểm khác nhau như hình, mỗi session kéo dài trong 3 giờ.



Hình 4. Hiệu quả khi áp dụng DNSBL

Kết quả thử nghiệm hiệu quả của cơ chế phòng chống đa lớp. Ta tiến hành giám sát hệ thống trong 6 tháng liên tiếp. Biểu đồ chỉ ra số lượng spam mail nhận được trước và sau khi triển khai cơ chế phòng chống. Mỗi session trong biểu đồ kéo dài trong 3 giờ. Kết quả trên biểu đồ cho thấy số lượng spam mail đã giảm đi từ 50% tới 60%, hệ thống không gặp phải tấn công DDoS trong suốt 6 tháng này.



Hình 5. Hiệu quả khi áp dụng cơ chế phòng chống đa lớp

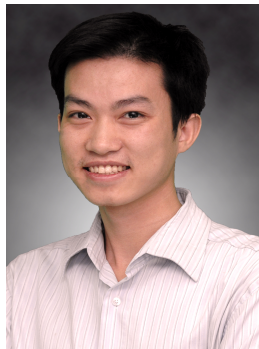
5. TỔNG KẾT

Trong bài báo này, chúng ta đã đưa ra cơ chế phòng chống đa lớp để phòng chống tấn công DDoS gây bởi spam. Bộ lọc nguồn đầu vào đã giúp chặn tấn công DDoS gây bởi spam. Bộ lọc nội dung chặn đứng spam bằng cách lọc các nội dung và chương trình không mong muốn. Việc giám sát mạng liên tục giúp người quản trị hiểu về cuộc tấn công và có đủ thời gian để phòng chống nó. Việc đào tạo người dùng giúp họ có được các hành động cần thiết đối với các cuộc tấn công, làm giảm đi ảnh hưởng của cuộc tấn công này. Các chính sách chặn spam mail bằng cách sử dụng các dấu hiệu nhận biết, không gửi mail hàng loạt và giới hạn việc sử dụng mail trong nhóm. Cuối cùng nhưng không kém quan trọng, đó là các giải pháp hợp lý giúp ngăn chặn tấn công. Thực tế kiểm nghiệm cho thấy đã giảm được 60% spam mail khi áp dụng cơ chế phòng chống đa lớp vào hệ thống.

6. TÀI LIỆU THAM KHẢO

1. Jae Yeon Jung, Emil sit: An empirical study of spam traffic and the use of DNS Black lists, ACM SIGCOMM Internet measurement conferences, pp 370-75.
2. Guangsen Zhang, Manish Parashar: Cooperative mechanism against DDOS attacks, SAM 2005, pg 86-96.
3. Anirudh Ramachandran, Nick Feamster: Understanding the network level behaviour of spammers, SIGCOMM 06.
4. Ben Adida, David Chau, Susan Hohenberger, Ronald L rivest: Lightweight Signatures for Email, DIMACS.
5. Vladimir Mijatovic: Mechanism for detecting and prevention of email spamming, Peer to Peer and SPAM in the Internet Raimo Kantola's technical report, 135-145.

Thông tin tác giả:



Âu Xuân Phong

Sinh năm: 1987.

Lý lịch khoa học: Tốt nghiệp Đại học ngành Điện tử Viễn Thông – Đại học Bách Khoa Hà Nội năm 2010.

Lĩnh vực nghiên cứu hiện nay: Nghiên cứu các giải pháp bảo mật, an ninh mạng và ứng dụng.

Email: phongax@ptit.edu.vn