HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Vũ Hoàng Anh

PHÂN TÍCH HÀNH VI VÀ MÔ HÌNH HÓA LAN TRUYỀN CỦA SÂU INTERNET

Chuyên ngành: Truyền dữ liệu và mạng máy tính

Mã số: 60.48.15

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI – 2013

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **PGS. TSKH Hoàng Đăng Hải**

Phản biện 1:

……

……

……

……

……

Phản biện 2:

……

……

……

……

……

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng .... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thô.

MỞ ĐẦU

Công nghệ thông tin là một trong những ngành phát triển trọng điểm của nhiều Quốc gia trên Thế giới bởi ứng dụng của nó. Cùng với công nghệ thông tin; mạng Internet cũng đã, đang và sẽ đóng góp rất nhiều trong công cuộc phát triển của xã hội loài người. Ngày nay mọi hoạt động của con người hầu như đều có thể thực hiện qua mạng Internet. Internet đã đem lại lợi ích cho nhiều người sử dụng, khai thác nó. Cùng với những lợi ích to lớn mà Internet đem lại; cũng nảy sinh những vấn đề phức tạp. Các thông tin cá nhân, thông tin kinh tế, chính trị và quân sự quan trọng của các tổ chức, các Quốc gia đều có nguy cơ bị lộ hoặc bị đánh cắp. Tài khoản ngân hàng bị đánh cắp, các hệ thống lưu trữ, cơ sở dữ liệu quan trọng bị tấn công, phá hoại… nhiều cuộc tấn công của các tin tặc đã gây thiệt hại hàng tỷ đô la.

Một trong những cách thức tấn công nguy hiểm của các tin tặc trên mạng Internet đó là dùng các loại sâu máy tính - worm. Sâu máy tính được kết hợp với một số kỹ thuật tấn công khác sẽ tạo ra một công cụ tấn công rất mạnh của các tin tặc. Chúng có thể tự động len lỏi tìm đến các mục tiêu (máy tính được nối mạng) và lấy cắp những thông tin từ mục tiêu này mà người sử dụng không biết gì. Vậy sâu máy tính là gì? Cách thức hoạt động của nó như thế nào? Vì sao nó có thể gây thiệt hại? Cách thức, công cụ phòng chống nó ra sao?. Xuất phát từ mong muốn được tìm hiểu về những hành vi và hoạt động cũng như cách thức phòng chống worm em thực hiện đề tài: “Phân tích hành vi và mô hình hóa lan truyền của sâu Internet”.

Phần nội dung

Chương 1: TỔNG QUAN VỀ SÂU INTERNET

1.1. Khái niệm sâu Internet

Worm – sâu máy tính (sau đây gọi tắt là sâu) được hiểu như là một loại virus đặc biệt hay một chương trình độc hại. Phương thức lây lan qua mạng là khác biệt cơ bản giữa virus và sâu. Hơn nữa, sâu có khả năng lan truyền như chương trình độc lập mà không cần lây nhiễm qua tập tin. Ngoài ra, nhiều loại sâu có thể chiếm quyền kiểm soát hệ thống từ xa thông qua các "lỗ hổng" mà không cần có sự "giúp sức" nào từ người dùng. Tuy nhiên, cũng có những trường hợp ngoại lệ như sâu Happy99, Melissa, LoveLetter, Nimda...

1.2. Quá trình phát triển

Cũng như công nghệ thông tin ngày nay sâu phát triển với tộc độ chóng mặt, cùng với các kỹ thuật tiên tiến và công nghệ hiện đại sâu đã có những bước phát triển vượt bậc. Sau đây là một cách nhìn về quá trình phát triển của sâu gồm 4 giai đoạn sau:

Thế hệ thứ nhất : (năm 1979 đến đầu những năm 1990).

Thế hệ thứ hai: (đầu những năm 1990 đến 1998

Thế hệ thứ ba: (từ 1999 đến 2000)

Thế hệ thứ tư: (từ 2001 đến nay)

1.3. Phân loại sâu Internet

1.3.1. Phân loại theo mục tiêu khám phá

Một con sâu muốn lây nhiễm vào một máy thì trước tiên nó phải tìm hiểu xem máy đó còn tồn tại trên mạng hay không. Một số kỹ thuật của sâu dùng để khám phá những sâu như vậy đó là: quét chủ động và quét thụ động. Đây chính là các loại sâu được phân loại theo mục tiêu khám phá những nạn nhân mới. Tuy vậy những con sâu có thể kết hợp các kỹ thuật khác nhau để đạt hiệu quả cao nhất trong lan truyền cũng như thực hiện mục đích của sâu.

1.3.1.1. Kỹ thuật quét chủ động

Sâu Internet có thể tự động tìm kiếm các nạn nhân bằng việc quét các địa chỉ được tạo ra một cách ngẫu nhiên hay có được tạo ra từ trước.

1.3.1.2. Kỹ thuật quét thụ động

Một con sâu kiểu thụ động không tự động tìm kiếm các nạn nhân. Thay vào đó hoặc là chúng chờ cho các nạn nhân tiềm năng liên lạc với chúng hoặc lợi dụng hành vi của người sử dụng để tìm đến các mục tiêu mới.

1.3.2. Phân loại theo phương tiện lan truyền và cơ chế phân phối

Những phương tiện lây nhiễm cũng có thể ảnh hưởng tới tốc độ và kỹ thuật tàng hình của một con sâu. Một con sâu có thể chủ động lây lan từ máy này sang máy khác, hoặc có thể được mang theo như là một phần của những giao tiếp bình thường.

1.3.2.1. Tự thực hiện

1.3.2.2. Kênh thứ hai

1.3.2.3. Nhúng

1.3.3. Phân loại theo đối tượng kích hoạt

Phương tiện kích hoạt sâu trên một host lưu trữ ảnh hưởng đáng kể tới việc lây nhiễm của sâu. Một vài sâu có thể được kích hoạt để lây nhiễm ngay lập tức, nhưng cũng có những sâu có thể phải chờ vài ngày hoặc vài tuần để được kích hoạt.

1.3.3.1. Kích hoạt bởi con người

1.3.3.2. Kích hoạt dựa vào hoạt động của con người

1.3.3.3. Quy trình kích hoạt theo lịch

1.3.3.4. Tự kích hoạt

1.3.4. Phân loại theo chức năng

Ngoài mục đích lan truyền trên Internet sâu còn có thể thực hiện các mục đích khác nhau phụ thuộc vào mục tiêu của cuộc tấn công hay ý định của kẻ viết ra sâu. Các loại sâu khác nhau sẽ thực hiện nhiệm vụ khác nhau của những kẻ tấn công.

1.3.4.1. Tạo lưu lượng giả

1.3.4.2. Điều khiển từ xa qua mạng Internet

1.3.4.3. Phát tán thư rác

1.3.4.4. Chuyển hướng trang web thông qua HTML-Proxies

1.3.4.5. Tấn công từ chối dịch vụ DOS qua Internet

1.3.4.6. Thu thập thông tin

1.3.4.7. Phá hủy dữ liệu

1.3.4.8. Điều khiển thiết bị vật lý từ xa

1.3.4.9. Tấn công lớp vật lý

1.3.4.10. Duy trì và cập nhật phiên bản mới

1.4. Ví dụ về một số loại sâu điển hình

1.4.1. Sâu Morris 1988

Sâu Morris là sâu đầu tiên được phát tán qua Internet. Tác giả của Morris là Robert Tappan Morris (hiện ông là giáo sư tại MIT), một sinh viên Đại học Cornell. Sâu Morris được thả lên mạng vào ngày 2 tháng 11 năm 1988 từ học viện MIT, nó được phát tán từ MIT để che dấu thực tế là con sâu này đã được bắt nguồn từ Cornell.

1.4.2. Sâu Melissa 1999

* *Kiến trúc, cách thức hoạt động của sâu Melissa:*

Sâu Melissa năm 1999 đã đánh vào tâm lý hiếu kỳ của phần đông người dùng Internet. Rất nhiều kẻ tò mò đã download một file có tên List.DOC từ diễn đàn "người lớn" khi tưởng rằng file này chứa các thông tin giúp họ truy cập miễn phí 80 trang web khiêu dâm. Họ đâu hay biết đã bị lây nhiễm một trong những sâu máy tính nguy hiểm nhất mọi thời đại.

1.4.3. Virus Code Red 2001

Code Red xuất hiện vào ngày 13/7/2001; lợi dụng một lỗi tràn bộ nhớ đệm trên các máy chủ IIS (Internet Information Server - tính năng của Windows cho phép người dùng tự lập một máy chủ web cá nhân.

1.4.4. Sâu Mydoom 2004

MyDoom xuất hiện (2004) có hơn 20 biến thể: Chỉ mất vài giờ (26/1/2004), "làn sóng" MyDoom đã có mặt trên toàn thế giới bằng phương thức phát tán truyền thông: qua email.

1.4.5. Storm worm 2007

Stom worm lợi dụng các lỗ hổng trong chương trình send mail và outlook để lan truyền trên Internet với tốc độ lớn vào giữa năm 2007

1.4.6. Stuxnet 2010

Stuxnet là một con sâu máy tính sống trong môi trường hệ điều hành Windows, khai thác triệt để những lỗ hổng của hệ điều hành này để phá hoại một mục tiêu vật chất cụ thể. Nó được tạo ra để hủy diệt một mục tiêu cụ thể như nhà máy điện, nhà máy lọc dầu hoặc nhà máy

hạt nhân sau khi bí mật xâm nhập hệ thống điều khiển quy trình công nghiệp, viết lại chương trình điều khiển này theo hướng tự hủy hoại.

1.5. Tình hình sâu Internet ở Việt Nam

Cơ sở hạ tầng máy tính và mạng cũng đã phát triển tại Việt Nam; Internet đóng một vai trò quan trọng trong nhiều lĩnh vực của đời sống xã hội và cũng là một bộ phận của mạng Internet toàn cầu. Trong lịch sử lây lan và tấn công của các sâu trên Internet; hệ thống mạng Việt Nam cũng không phải là một ngoại lệ như: Ngày 12/8/2003 sâu W32.Blaster.Worm bắt đầu tràn vào Việt nam trong khi nó bắt đầu phát tán trên toàn cầu vào ngày 11/8/2003. Các sâu Code Red hay Slammer cũng lây lan vào mạng Việt Nam thông qua hệ thống email...

1.6. Tóm tắt chương

Chương 1 đã trình bày khái niệm và các đặc trưng cơ bản của sâu Internet. Các loại sâu đã được phân loại theo các tiêu chí gồm: mục tiêu khám phá, phương tiện lan truyền và cơ chế phân phối, chức năng hay hành vi tấn công. Chương đã giới thiệu một số sâu điển hình, tình hình phát triển của sâu Internet tại Việt Nam.

Chương 2: MÔ HÌNH HÓA LAN TRUYỀN CỦA SÂU INTERNET

2.1. Các chu trình của sâu Internet

2.1.1. Mô hình lan truyền theo kiểu bệnh dịch

Virus máy tính và worms giống như virus sinh học ở hành vi nhân bản và lây lan của chúng. Những thuật toán được phát triển cho việc nghiên cứu những bệnh truyền nhiễm có thể được điều chỉnh cho phù hợp với việc nghiên cứu virus máy tính và sự lan truyền của worm.

2.1.1.1. Mô hình bệnh dịch cổ diển đơn giản

Trong mô hình dịch bệnh cổ điển đơn giản [4], mỗi máy chủ ở một trong hai trạng thái: dễ bị lây nhiễm hoặc truyền nhiễm. Mô hình giả định rằng một máy khi đã bị virus lây nhiễm, thì nó sẽ ở trạng thái truyền nhiễm mãi mãi. Chính vì vậy sự biến đổi của bất kỳ máy nào cũng chỉ có thể từ dễ bị lây nhiễm sang trạng thái truyền nhiễm.

2.1.1.2. Mô hình bệnh dịch tổng quát Kermack-Mckendrick

Trong lĩnh vực dịch tễ học, mô hình Kermack-Mckendrick [4] xem xét quá trình loại bỏ những máy đã bị lây nhiễm. Nó giả định rằng trong một đại dịch của một bệnh dịch truyền nhiễm, một vài máy lây nhiễm hoặc được phục hồi hoặc là chết; một máy được phục hồi từ máy đã chết, nó sẽ được miễn dịch với bệnh mãi mãi – những máy được trong trạng thái loại bỏ sau khi chúng được phục hồi hoặc chết do bệnh dịch. Do vậy mỗi máy chỉ có thể ở một trong 3 trạng thái tại mọi thời điểm: dễ bị lây nhiễm, lây nhiễm và bị loại bỏ. Bất kỳ máy nào trong hệ thống hoặc chuyển từ trạng thái "dễ bị lây nhiễm lây nhiễm bị loại bỏ" hoặc trong trạng thái "dễ bị lây nhiễm" mãi mãi.

2.1.2. Mô hình lan truyền hai thành tố

Quá trình lan truyền thực sự của sâu trên Internet là một quá trình phức tạp. Trong phần này, bài sẽ chỉ đề cấp tới những sâu được liên tục kích hoạt. Theo cách này, một sâu trên một máy truyền nhiễm liên tục cố gắng tìm kiếm và lây nhiễm cho những máy có nguy cơ lây nhiễm, giống sự cố của sâu Code Red vào ngày 19 tháng 7 năm 2011.

2.1.2.1. Hai yếu tố ảnh hưởng tới sự lan truyền của Sâu Internet (Code Red worm)

Qua việc phân tích lan truyền của sâu Code Red; thấy rằng có hai yếu tố không xuất hiện trong mô hình theo kiểu dịch bệnh. Hai yếu tố này ảnh hưởng tới quá trình lan truyền của Code Red:

+ Kết quả các biện pháp đối phó của con người trong việc loại bỏ cả hai máy tính đã lây nhiễm và máy dễ bị lây nhiễm. Số lượng người dân nhận thức về mức độ nguy hiểm của

Code Red ngày càng gia tăng và họ thực hiện các biện pháp đối phó như: làm sạch máy tính bị nhiễm, vá hoặc nâng cấp phần mềm bảo vệ cho máy dễ bị lây nhiễm, thiết lập bộ lọc để ngăn chặn lưu lượng truy cập sâu trong tường lửa hoặc bộ định tuyến biên, thậm chí họ còn ngắt cả kết nối Internet.

+ Tỷ lệ nhiễm (t) giảm xuống chứ không phải là một tỷ lệ không đổi. Code Red lan truyền với quy mô lớn trong Internet rộng lớn đã làm ùn tắc và các thiết bị định tuyến trên Internet cũng bị quá tải, do đó chính việc quét của Code Red cũng đã bị chậm lại.

2.1.2.2. Mô hình hai thành tố

Như chúng ta thấy việc lan truyền của worm là một quá trình rời rạc. Tuy nhiên để mô hình hóa lan truyền của sâu Internet thì việc sử dụng phương trình vi phân liên tục cũng cho kết quả gần đúng. Phương trình vi phân liên tục sử dụng phù hợp cho quá trình lan truyền trên diện rộng với quy mô mạng lớn như Internet.

2.2. Phân tích mô hình hai thành tố trong lan truyền của Code Red worm

Quá trình loại bỏ từ máy chủ dễ bị lây nhiễm phức tạp hơn trong mô hình Kermack-McKendrick. Vào lúc bắt đầu lan truyền của sâu; hầu hết mọi người đều chưa biết về sự tồn tại của Code Red worm. Kết quả là việc loại bỏ những máy nhạy cảm là nhỏ và tăng chậm. Khi có nhiều và nhiều hơn nữa những máy tính bị nhiễm bệnh, con người đã có nhận thức về Code Red worm và tầm quan trọng của việc chống lại nó. Do đó tốc độ tiêm chủng tăng nhanh trong thời gian tiếp theo đó. Tốc độ giảm khi số lượng máy nhạy cảm co lại và hội tụ về không khi không có máy nhạy cảm nào.

2.3. Tóm tắt chương

Chương 2 đã trình bày và phân tích về mô hình hóa lan truyền của sâu Internet. Luận văn tập trung vào phân tích hai mô hình điển hình là lan truyền kiểu bệnh dịch và lan truyền hai thành tố.

Quá trình lan truyền thực sự của sâu trên Internet là một quá trình phức tạp. Mặt khác, các biện pháp đối phó của con người đóng vai trò quan trọng trong việc bảo vệ và chống lại sâu Internet. Do vậy, việc mô hình hóa lan truyền của sâu Internet là một việc hết sức khó khăn. Các mô hình ngẫu nhiên và xác định trong lĩnh vực dịch tễ học có thể sử dụng để mô hình hóa sự lan truyền của sâu Internet như kiểu lan truyền lây nhiễm bệnh dịch cổ điển. Tuy

nhiên, các mô hình này cũng không thể hoàn toàn phù hợp cho mô hình hóa lan truyền của sâu Internet, đòi hỏi phải có sự điều chỉnh phù hợp.

Chương 3: MÔ HÌNH VÀ KỸ THUẬT PHÒNG CHỐNG WORM

3.1. Các kỹ thuật phát hiện worm

Cùng với sự phát triển của các kỹ thuật trong mô hình của sâu các kỹ thuật nhằm phát hiện và phòng chống sâu Internet cũng đã được nghiên cứu và áp dụng. Sau đây là một vài kỹ thuật phát hiện worm dựa vào việc phân tích lưu lượng truyền thông, giám sát những cổng nhạy cảm, những lỗ hổng của hệ thống và phát hiện dựa vào định danh. Những phương pháp này là những phương pháp quan trọng và cốt lõi để phát hiện Hacker và đặc biệt là sâu Internet.

3.1.1. Phân tích lưu lượng

Phương pháp phân tích lưu lượng đã được phát triển để theo dõi các Hacker, phương pháp này cũng đã được áp dụng để thiết kế và thực hiện trong nhiều phần mềm theo dõi và giám sát hoạt động của sâu; vì vậy nó cũng đáng tin cậy.

3.1.2. Giám sát những hố đen trong mạng và những cổng nhạy cảm

Hai phương pháp hiệu quả để xác định sâu mạng và theo dõi hành vi của chúng là sử dụng hệ thống giám sát hố đen và những cổng nhạy cảm. Các hệ thống này có khả năng theo dõi hành vi của sâu và ghi lại những gì quan sát được. Những phân tích dữ liệu sau đó sẽ mang lại những manh mối có giá trị như tốc độ tăng trưởng của sâu, hoặc thậm chí cả sự hiện diện của những agent mới xâm nhập vào mạng.

3.1.2.1. Honeypots

3.1.2.2. Giám sát hố đen

Phương pháp theo dõi sâu không cần sử dụng không gian IP đã được chứng minh là có hiệu quả trong việc theo dõi và phát hiện sâu.

3.1.3. Phát hiện dựa vào định danh

Mô hình phát hiện worm dựa vào định danh sử dụng cơ sở dữ liệu bao gồm các thông tin về những con sâu đã được biết đến trước đó để đối chiếu với kẻ lạ mặt xâm nhập vào hệ thống từ đó đưa ra các cảnh báo về một con sâu. Có ba loại chính của hệ thống phát hiện dựa vào định danh.

3.1.3.1. Mô hình truyền thống trong phân tích định danh

Phân tích định danh là phương pháp phân tích nội dung của dữ liệu bị bắt để phát hiện sự hiện diện của những chuỗi đã được biết đến. những chữ ký được lưu trữ trong cơ sở dữ liệu và đã được chỉ ra từ nội dung của những file độc hại được biết đến. Những file này thường là những chương trình thực thi được kết hợp với sâu.

3.1.3.2. Phân tích định danh tải trọng mạng

Bởi vì sâu tồn tại thông qua các hoạt động mạng, sự hiện diện của chúng có thể được phát hiện bằng các sử dụng bộ giám sát mạng thụ động và bộ giám sát định danh tải trọng. Worm thường có những định danh đặc biệt khi chúng tấn công các máy chủ trên mạng. Bằng cách xây dựng thư viện những định danh độc hại được biết đến, một bộ giám sát mạng có thể cảnh báo cho một quản trị viên biết về sự xuất hiện của một hoạt động bất thường và của một worm mạng.

3.1.3.3. Phân tích định danh logfile

Nhiều sâu tấn công tất cả các máy chủ mà không có sự chọn lọc có thể bị phát hiện bằng việc triển khai các máy chủ có hệ thống an ninh tốt. Khi các con sâu đó tấn công các máy chủ đó không hề bị tổn thương; ngược lại chúng còn thu thập được thông tin về con sâu đó như: tải trọng, kích thước hay máy nguồn của sâu … tất cả các thông tin này đều được lưu trong file log của máy chủ đó. Việc phân tích những thông tin trong file log đó có thể cho chúng ta những định danh về một con sâu. Từ đó có thể cập nhật cho các máy chủ khác biết về chúng và loại trừ hay ngăn chặn những yêu cầu của các sâu.

3.1.3.4. Phân tích định danh file

Kiểm tra nội dung của một hệ thống file chúng có thể được sử dụng để phát hiện sự có mặt của một con sâu. Bởi vì hầu hết các sâu đều thực thi nhị phân và đều nằm trên ổ đĩa của hệ thống. Đây là phương pháp phổ biến nhất được sử dụng để tìm kiếm sâu, và cũng là cơ sở cho việc cài đặt các phần mềm antivirus. Để kiểm tra sự hiện diện của sâu, một công cụ phát hiện sâu sẽ được thực thi để quét bộ nhớ của hệ thống.

3.2. Một số mô hình phòng chống worm

Phòng chống sâu Internet là một công việc được các nhà an ninh mạng quan tâm vì thiệt hại do sâu Internet gây ra là rất lớn. Đã có nhiều nghiên cứu, đề xuất về mô hình và phương pháp để phòng chống sâu. Phần sau đây sẽ giới thiệu mô hình điển hình là "Friends Model".

3.2.1. Mô hình Friends

Mô hình (tạm dịch là mô hình bè bạn) này dựa trên sự sẵn sàng hợp tác của các máy chủ trên giao thức được sắp xếp từ trước. Khi một con sâu được phát hiện lập tức nó sẽ được

thông báo đến tất cả các máy trong mạng bởi một giao thức. Cảnh bảo này có thể được gửi đi từ một máy dò toàn cục hay từ một máy dò của một tập hợp các máy chủ tham gia hệ

thống. Điều này còn phụ thuộc vào khả năng của máy dò. Mục tiêu của phương pháp này là tối đa hoá các máy chủ được bảo vệ khỏi sâu.

3.3. Một số công cụ phòng chống worm

3.3.1. Công cụ Kuang

Kuang là một hệ thống dựa vào những quy tắc; nó tìm ra những mâu thuẫn trong thiết lập của các quyết định bảo vệ được thực hiện bởi người sử dụng và người quản trị của một hệ thống UNIX. Nó cho phép người quản lý hệ thống thực hiện phân tích điều gì sẽ xảy ra trong tương lai của một cấu hình bảo vệ, và trong chế độ đó nó giúp người quản lý tạo ra những quyết định bảo vệ. Công cụ Kuang ngầm định rằng khi đã truy cập được vào hệ thống thì có thể trở thành chủ nhân của hệ thống đó. Với một tập các đặc quyền ban đầu và mục tiêu cuối cùng, thệ thống này phân tích cấu hình bảo vệ và đưa ra thứ tự những bước thực hiện những công việc để đạt được những mục tiêu cuối cùng đó nếu có thể.

3.3.2. Công cụ NetKuang

NetKuang [7] là phần mở rộng của Kuang. Nó chạy trên mạng của những máy tính sử dụng UNIX và có thể tìm thấy lỗ hổng được tạo ra bởi những cấu hình hệ thống yếu kém ở mức độ mạng cho phép kẻ tấn công có nhảu từ một hệ thống sang các hệ thống khác. Lỗ hổng được phát hiện bằng cách tìm kiếm dựa trên mục tiêu ban đầu; đó là trên một host và song song khi nhiều hosts được kiểm tra.

3.3.3. Công cụ NOOSE

NOOSE (Networked Object-Oriented Security Examiner) [7] là một hệ thống phân tích lỗ hổng phân tán dựa trên mô hình đối tượng. Nó kết hợp máy quét của host và của mạng, lưu trữ các kết quả vào trong mốt số lớp đối tượng. Nó có thể thu thập các lỗ hổng bảo mật từ nhiều nguồn khác nhau, bao gồm cả các kết quả đầu ra của các chương trình phân tích khác. NOOSE trình bày các thông tin về lỗ hổng như một cơ sở dữ liệu tích hợp, và dễ dàng cho việc tích hợp vào chuỗi kết của từ nhiều tài khoản và hệ thống khác.

3.3.4. Các công cụ khác

Có nhiều biện pháp, công cụ của nhiều hãng khác nhau nhằm bảo mật hệ thống một cách tốt nhất. Một vài hệ thống bảo mật tốt nhất được PC World Mỹ phối hợp cùng AV-Test.org thực hiện đợt "sát hạch", đánh giá vào năm 2012 là những hệ thống sau:

G-DATA InternetSecurity 2012, Norton Internet Security 2012, Bitdefender Internet Security 2012, Kaspersky Internet Security 2012, Trend Micro Maximum Security 2012.

3.4. Tóm tắt chương

Trên cơ sở những phân tích trong chương 2 về hành vi, mô hình hóa các đặc trưng lan truyền của sâu Internet, Chương 3 của luận văn trình bày về mô hình và các kỹ thuật phòng chống sâu Internet. Nội dung chương tập trung vào các kỹ thuật phát hiện sâu Internet như phân tích lưu lượng, giám sát hố đen địa chỉ IP; một số mô hình và công cụ phòng chống sâu Internet điển hình đã có tới nay.

Chương 4: MỘT SỐ KẾT QUẢ MÔ PHỎNG THỬ NGHIỆM

Chương 1 của luận văn đã nghiên cứu tổng quan về sâu Internet, phân tích hành vi và cơ chế lan truyền của sâu Internet. Mô hình hóa quá trình lan truyền của sâu Internet đã được trình bày và phân tích trong chương 2. Chương 3 đã trình bày về các kỹ thuật phát hiện và một số mô hình, công cụ phòng chống sâu Internet. Nội dung chương 4 sẽ trình bày một số kết quả mô phỏng thử nghiệm khả năng phát hiện sâu Internet thông qua bộ công cụ mô phỏng NeSSi2. Trong phần tiếp theo, luận văn sẽ lần lượt giới thiệu về bộ công cụ, khả năng sử dụng để mô phỏng tấn công mạng, trình bày mô hình và kịch bản mô phỏng phát hiện sâu Internet với NeSSi2.

4.1. Công cụ sử dụng cho mô phỏng sâu Internet

4.1.1. Giới thiệu về bộ công cụ mô phỏng NeSSi2

NeSSi2 là một bộ công cụ mô phỏng tấn công mạng mới được phát triển tại Trường Đại học TU Berlin (CHLB Đức) từ vài năm nay. Luận văn sử dụng bộ công cụ này để thực hiện mô phỏng do khả năng mô phỏng hiệu quả của nó.

4.1.2. Các thành phần của bộ công cụ NeSSi2

4.1.2.1. Giao diện người dùng

4.1.2.2. Thành phần cốt lõi của bộ công cụ mô phỏng (Simulation Backend)

4.2.1.3. Cơ sở dữ liệu (Database).

4.2. Quy trình tạo và thực hiện kịch bản mô phỏng sâu Internet

4.2.1. Thiết lập mạng.

4.2.2. Thiết lập Profile

4.2.3. Thiết lập kịch bản mô phỏng

4.2.4. Thiết lập phiên kịch bản

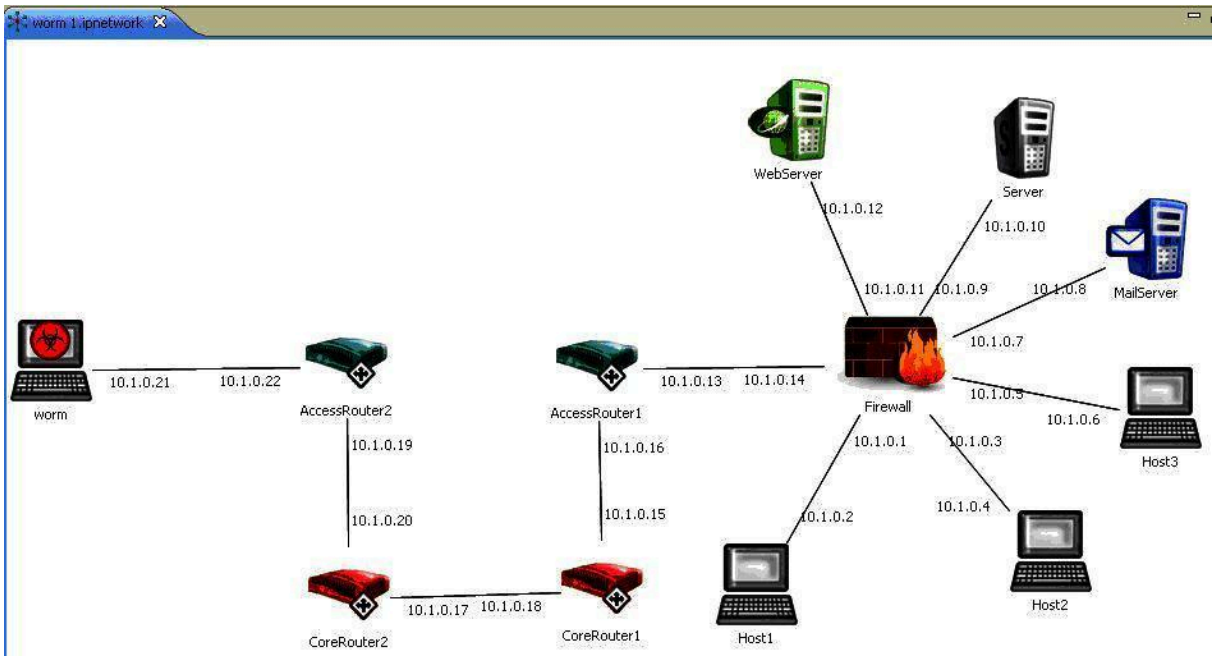
4.2.5. Thực hiện mô phỏng

4.3. Mô hình và kịch bản mô phỏng sâu Internet với NeSSi2

4.3.1. Sơ đồ mạng mô phỏng, chức năng các thành phần

**** Sơ đồ mạng cơ bản:***

Với mô phỏng quá trình quét tìm kiếm các host của sâu Code Red; ở đây chỉ sử dụng mô hình mạng cơ bản với số lượng host hạn chế. Trọng tâm của việc mô phỏng là theo dõi lưu lượng mạng, số lượng các gói tin được gửi tới các host và các server trong quá trình quét của sâu Inetetnet.



Hình 4.10: Sơ đồ mạng cơ bản dùng trong mô phỏng.

**** Các thành phần cơ bản trong mạng mô phỏng:***

- worm: một host truyền nhiễm.

- AccessRouter2: Router biên của nhà cung cấp dịch vụ.

- CoreRouter1, 2: Các bộ định tuyến của các mạng.

- AccessRouter1: Router biên của mạng.

- Firewall: Tường lửa của mạng.

- Host1, Host2, Host3: Các host đang online trong mạng.

- Server, Webserver, MailServer: Các server dịch vụ.

- Các đường nối giữa hai thiết bị bất kỳ: Các kết nối giữa các thiết bị trong mạng.

4.3.2. Tạo nguồn lưu lượng

Để tạo nguồn lưu lượng cho việc mô phỏng; cần thiết lập các profile và các tham số của chúng thực hiện chức năng, nhiệm vụ của mỗi thành phần trong mạng. Trong bài sử dụng Profile cho sâu có các thông số giống như một sâu Code Red.

4.3.3. Kịch bản mô phỏng

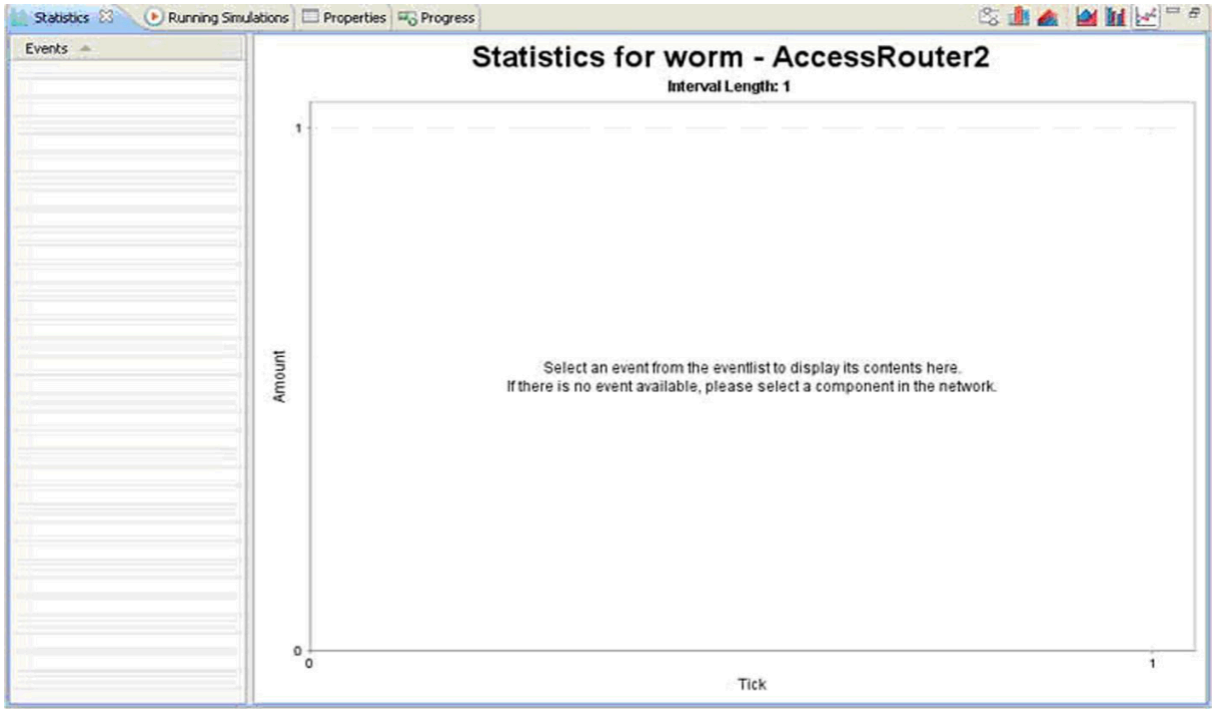
Kịch bản 1: Đo lưu lượng mạng gia tăng khi mạng chưa xuất hiện sâu Code Red.

Kịch bản 2: Mô phỏng quá trình quét, thu thập và vẽ biểu đồ về lưu lượng gia tăng của mạng khi sâu Code Red bắt đầu quét.

4.3.4. Các kết quả mô phỏng

4.3.4.1. Kịch bản 1: Mạng chưa bị lây nhiễm sâu Code Red

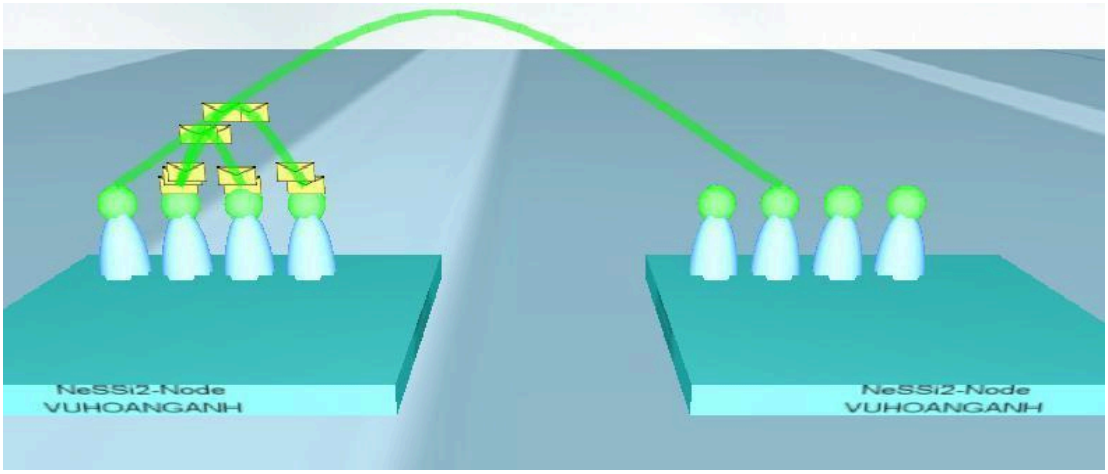
Để đo lưu lượng mạng gia tăng khi mạng chưa xuất hiện sâu Code Red; mạng được thiết lập bình thường chưa có các ứng dụng profile cho worm cũng như các thành phần khác trong mạng.



Hình 4.11: Trạng thái lưu lượng mạng khi chưa xuất hiện sâu Code Red.

4.3.4.2. Kịch bản 2: Sâu bắt đầu quét trong mạng

- Hình 4.12 mô tả bằng hình ảnh các gói tin được gửi bởi worm tới các host.

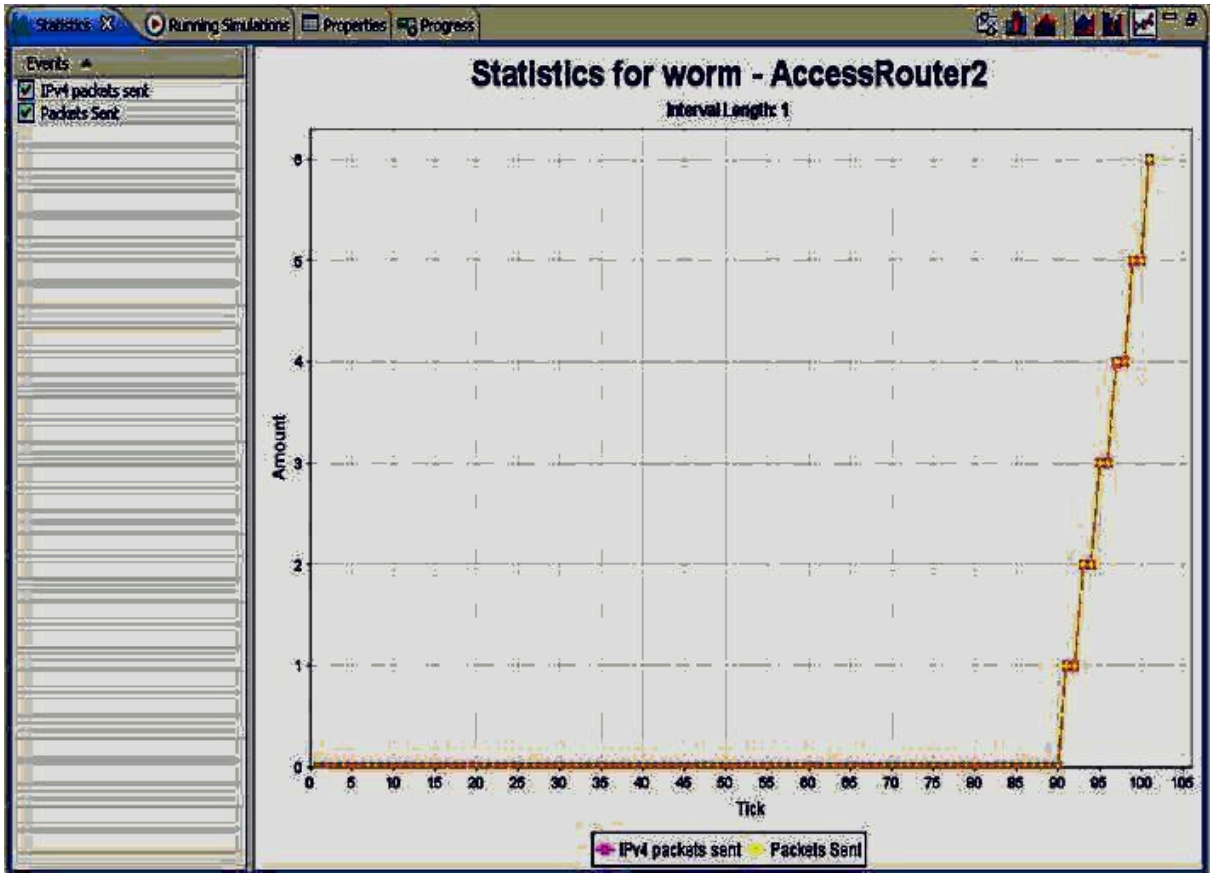


Hình 4.12: Các gói tin được gửi bởi worm tới các host.

Hình 4.12 được thực hiện khi sử dụng phần mềm Advanced Structured Graphical Agent Realm Display (ASGARD) truy xuất dữ liệu mô phỏng từ phần mềm NeSSi2. Hình

thể hiện các đối tượng trong mạng và quá trình gửi cũng như nhận gói tin giữa các thành phần trong mạng. Ở đây các gói tin được gửi từ worm tới các host và các server một cách liên tục và ngày càng gia tăng.

- Dưới đây là biểu đồ thể hiện số lượng các gói tin mà sâu Code Red đã gửi qua AccessRouter2



Hình 4.13: Các gói tin gửi tới các Host.

Trong hình 4.13: có hai loại gói tin là IP4 packet và packet được gửi đi bởi worm. Tại thời điểm t = 90 (tick) các gói tin đã bắt đầu được gửi đi. Lúc này sâu đã khởi tạo và thiết lập được gải địa chỉ IP để thực hiện quá trình quét. Số gói tin được gửi đi tăng rất nhanh. Mỗi khi các host nhận được các gói tin của sâu thì các host này lại gửi phản hồi lại ngược trở lại. Mỗi host khi đã bị sâu phát hiện và lây nhiễm lại trở thành một con sâu và bắt đầu thực hiện quá trình quét và lây nhiễm trong mạng.

- Theo dõi lưu lượng tại các host thấy rằng số lượng các gói tin mà các host phải nhận từ quá trình quét của sâu tăng đột biến kể từ khi sâu tìm thấy host đang online trên mạng.

4.4. Nhận xét, đánh giá

Việc mô phỏng sâu là một vấn đề rất khó bởi nhiều yếu tố như môi trường mạng thực tế luôn biến đổi như các hệ thống bảo mật và các host cũng như server luôn được cập nhật các phần mềm bảo vệ, sâu luôn được duy trì và cập nhật phiên bản mới… Luận văn cũng đã sử dụng công cụ NeSSi2 để mô phỏng quá trình quét của sâu Code Red. Do đặc điểm của bổ công cụ nên sâu Code Red, cũng như các thiết đặt của các thành phần mạng là ít được cập nhật như trong thực tế. Chính vì vậy mô phỏng phần nào đánh giá được mức độ lây lan của sâu nhưng không có được độ chính xác tuyệt đối so với thực tế.

KẾT LUẬN

Sâu Internet là một loại hình tấn công nguy hiểm do sự lan truyền nhanh chóng, sức tàn phá rộng khắp và những hậu quả nặng nề do nó mang lại cho cộng đồng mạng.

Kỹ thuật sản sinh sâu, lây lan và tấn công… ngày càng tinh vi, phức tạp cùng với sự phát triển của công nghệ mới. Do đó, việc nghiên cứu, phân tích hành vi, mô hình hóa lan truyền của sâu Internet là một điều khó khăn, có nhiều thách thức.

Mong muốn của luận văn là nghiên cứu tìm hiểu bản chất của sâu, cách thức hoạt động, khả năng và phương thức lây lan, hành vi và hoạt động của chúng để có thể mô hình hóa, đưa ra các biện pháp phòng chống, ngăn chặn có hiệu quả.

Luận văn đã đạt được các mục tiêu nghiên cứu đề ra, cụ thể gồm:

+ Nghiên cứu bản chất của sâu Internet, phân loại, phân tích hành vi và cơ chế lan truyền của chúng, trình bày 1 số loại sâu điển hình.

+ Mô hình hóa quá trình lan truyền của sâu Internet dựa theo 2 mô hình lây nhiễm cổ điển và mô hình sâu hai thành tố.

+ Nghiên cứu về mô hình và các kỹ thuật phát hiện, phòng chống và ngăn chặn sâu Internet dựa trên các kỹ thuật phân tích lưu lượng, sử dụng bẫy như Honeypot/Honeynet, kỹ

thuật giám sát hố đen địa chỉ IP, một số mô hình và công cụ phát hiện, phòng chống sâu.

+ Đề xuất mô hình mô phỏng thử nghiệm sâu Internet với bộ công cụ mô phỏng NeSSi2. Xây dựng mạng mô phỏng, kịch bản mô phỏng thử nghiệm tấn công và phát hiện sâu Internet.

DANH MỤC CÁC TÀI LIỆU THAMKHẢO

Tiếng Việt

[1] Nguyễn Xuân Hoài (1999), *Tập bài giảng môn học Virus máy tính*, Học viện kỹ thuật Quân sự.

[2] Ngô Anh Vũ (2005), *Virus huyền thoại hay thực tế*, NXB Tổng hợp TP. Hồ Chí Minh.

Tiếng Anh

[3] Markus Kern. Re: Codegreen beta release, http://online.securityfocus.com/archive/82/211462.

[4] C. C. Zou, W. Gong, and D. Towsley (2002), *Code Red Worm Propagation Modeling and Analysis*, in 9th ACM Conference on Computer and Communication Security

[5] K. Eichman. Mailist (2001); *Possible CodeRed Connection Attempts*. http://lists.jammed.com/incidents/2001/07/0159.html

[6] Jose Nazario (2004), *Defense and Detection Strategies against Internet Worms*, Artech house, inc.

[7] SG Cheetancheri (2004), *Modelling a Computer Worm Defense System* , seclab.cs.ucdavis.edu