BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

NGUYỄN HOÀNG NAM

XÂY DỰNG TÍNH NĂNG CẢNH BÁO TẤN CÔNG TRÊN MÃ NGUỒN MỞ

LUẬN VĂN THẠC SĨ

Chuyên ngành : Công nghệ thông tin

Mã số ngành : 60480201

TP. HỒ CHÍ MINH, tháng 10 năm 2014

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

NGUYỄN HOÀNG NAM

XÂY DỰNG TÍNH NĂNG CẢNH BÁO TẤN CÔNG TRÊN MÃ NGUỒN MỞ

LUẬN VĂN THẠC SĨ

Chuyên ngành : Công nghệ thông tin

Mã số ngành : 60480201

CÁN BỘ HƯỚNG DẪN KHOA HỌC: TS. LÊ MẠNH HẢI

TP. HỒ CHÍ MINH, tháng 10 năm 2014

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

Cán bộ hướng dẫn khoa học : TS. LÊ MẠNH HẢI

(Ghi rõ họ, tên, học hàm, học vị và chữ ký)

Luận văn Thạc sĩ được bảo vệ tại Trường Đại học Công nghệ TP. HCM ngày … tháng 10 năm 2014

Thành phần Hội đồng đánh giá Luận văn Thạc sĩ gồm:

(Ghi rõ họ, tên, học hàm, học vị của Hội đồng chấm bảo vệ Luận văn Thạc sĩ)

TT	**Họ và tên**	**Chức danh Hội đồng**
		Chủ tịch
		Phản biện 1
		Phản biện 2
		Ủy viên
		Ủy viên, Thư ký

Xác nhận của Chủ tịch Hội đồng đánh giá Luận sau khi Luận văn đã được sửa chữa (nếu có).

Chủ tịch Hội đồng đánh giá LV

TRƯỜNG ĐH CÔNG NGHỆ TP. HCM

PHÒNG QLKH – ĐTSĐH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

TP. HCM, ngày…. tháng10 năm 2014

NHIỆM VỤ LUẬN VĂN THẠC SĨ

Họ tên học viên: NGUYỄN HOÀNG NAM.....Giới tính: Nam ...

Ngày, tháng, năm sinh: 02-02-1982.....Nơi sinh: TPHCM

Chuyên ngành: Công nghệ thông tin.....MSHV: 1241860012.

I- Tên đề tài:

XÂY DỰNG TÍNH NĂNG CẢNH BÁO TẤN CÔNG TRÊN MÃ NGUỒN MỞ.....

.....

.....

II- Nhiệm vụ và nội dung:

Xây dựng tính năng phát hiện và cảnh báo tấn công trên mã nguồn mở Nagios nhằm chủ động hơn trước các các tấn công từ chối dịch vụ .....

.....

.....

.....

III- Ngày giao nhiệm vụ: *02-04-2014*

IV- Ngày hoàn thành nhiệm vụ: 20/09/2014 .....

V- Cán bộ hướng dẫn: TS. LÊ MẠNH HẢI .....

.....

.....

CÁN BỘ HƯỚNG DẪN

(Họ tên và chữ ký)

KHOA QUẢN LÝ CHUYÊN NGÀNH

(Họ tên và chữ ký)

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các số liệu, kết quả nêu trong Luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tôi xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện Luận văn này đã được cảm ơn và các thông tin trích dẫn trong Luận văn đã được chỉ rõ nguồn gốc.

Học viên thực hiện Luận văn

(Ký và ghi rõ họ tên)

Nguyễn Hoàng Nam

LỜI CÁM ƠN

Để hoàn thành luận văn này, tôi xin chân thành cảm ơn Thầy TS. Lê Mạnh Hải đã tận tình hướng dẫn, chỉ bảo và giúp đỡ trong suốt thời gian thực hiện đề tài. Tôi bày tỏ lòng biết ơn Ban chủ nhiệm khoa CNTT Trường Đại học Công Nghệ TPHCM đã hỗ trợ để tôi hoàn thành luận văn này.

Nguyễn Hoàng Nam

TÓM TẮT

An ninh mạng là một vấn đề đáng lo ngại trong thời đại hiện nay. Hệ thống mạng luôn đứng trước các nguy cơ tấn công gây thiệt hại lớn, không cảnh báo trước của tin tặc. Để giúp cho công việc đảm bảo an ninh của hệ thống mạng được nâng cao, cần có một giải pháp dò tìm, phát hiện các dấu hiệu tấn công và cảnh báo kịp thời.

Luận văn này tập trung xây dựng tính năng cảnh báo tấn công trên nền tảng mã nguồn mở Nagios. Đây là công cụ hỗ trợ giám sát mạng rất hữu hiệu. Ưu điểm của Nagios chính là tính mở, cho phép người dùng có thể chỉnh sửa, bổ sung thêm những tính năng cần thiết mới. Tính năng phát hiện tấn công được xây dựng trên thuật toán phát hiện các dấu hiện bất thường của giao thức hướng kết nối TCP. Thuật toán này rất đơn giản, dễ dàng cài đặt so với các thuật toán khác có chức năng tương tự. Tuy nhiên lại rất hiệu quả trong việc phát hiện các dấu hiệu tấn công với cường độ lớn, với nhiều kỹ thuật tấn công đa dạng. Ngay khi có các dấu hiệu bất thường xảy ra, tín hiệu cảnh báo trên Nagios sẽ được thiết lập và gửi đến người quản trị.

Dựa vào kết quả này, người quản trị viên sẽ chủ động hơn trước các tình huống tấn công nguy hiểm, có được các biện pháp đối phó hợp lý và khắc phục sự cố trong thời gian sớm nhất.

ABSTRACT

Network security is an issue of concern in the current era. Networking has always against the risk causing by hackers. To improve network security, a best solution to scan, detect signs of attack is neccessary.

This thesis focused on building an attack alert feature on an open source platform, Nagios. This is one of the best network monitoring tool. Advantages of Nagios is an open source allowing users to edit, add new features easily. Attack detection features was built on abnormal TCP connection-oriented protocol detection algorithm. It is very simple and easy to install. It is used to detect large attacks with multiple techniques effectively. Nagios will send an alert to aministrator if something missmatches.

Base on these results, administrator will get more proactive with dangerous atacks. They can solve every problems as soon as the first phase of the attacks.

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

ACK	Acknowledgement
CGI	Common Gateway Interface
Client	Máy khách
CPU	Central Unit Proccessing

DDoS	Distributed Denial of Service
DNS	Domain Name Service
DoS	Denial of Service
DRDoS	Distributed Reflection Denial of Service
FIN	Finish
FTP	File Transfer Protocol
Hacker	Tin tặc
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MIB	Management Information Base
MRTG	Multi Router Traffic Grapher
NRPE	Nagios Remote Plugin Excecutor
OID	Object Identifier
Peer-to-Peer	Mạng ngang hàng
POP3	Post Office Protocol 3
RAM	Random Access Memory
RTO	Retransmission Timeout
RTT	Round Trip Time
Server	Máy chủ
SMTP	Simple Mail Transer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SYN	Synchronize

TCP	Transmission Contrlo Protocol
UDP	User Datagram Protocol

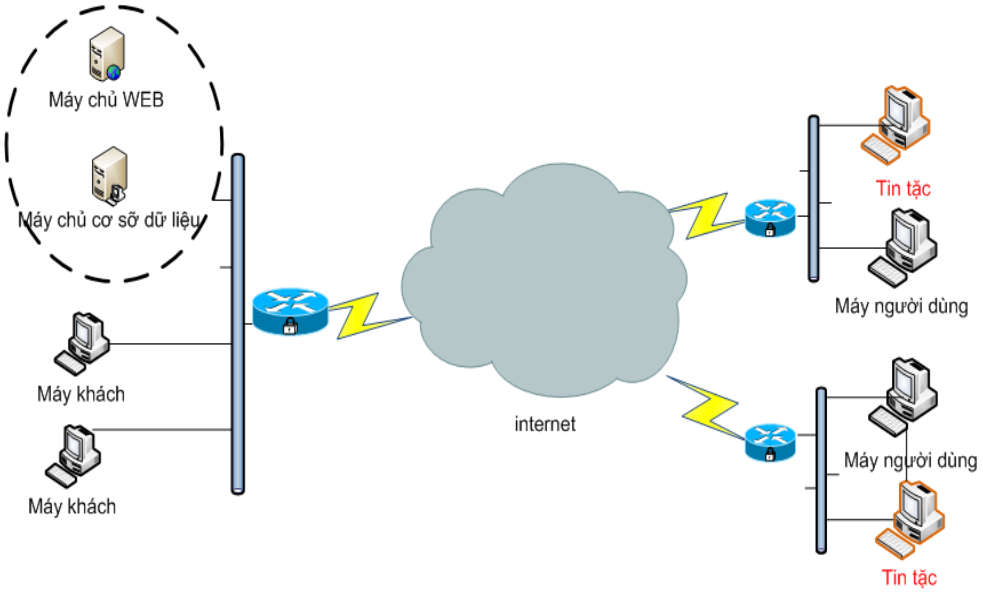
DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG

CHƯƠNG 1: GIỚI THIỆU

1.1 Đặt vấn đề

Hệ thống máy tính bao gồm nhiều thiết bị kết nối với nhau, mỗi thiết bị khác nhau được sản xuất bởi nhiều hãng khác nhau như: máy chủ, bộ lưu trữ, các thiết bị mạng…Các dịch vụ được triển khai trên hệ thống, nhằm đáp ứng nhu cầu sử dụng của người dùng, cần mức tối thiểu tài nguyên trên các thiết bị để có thể hoạt động được tốt.

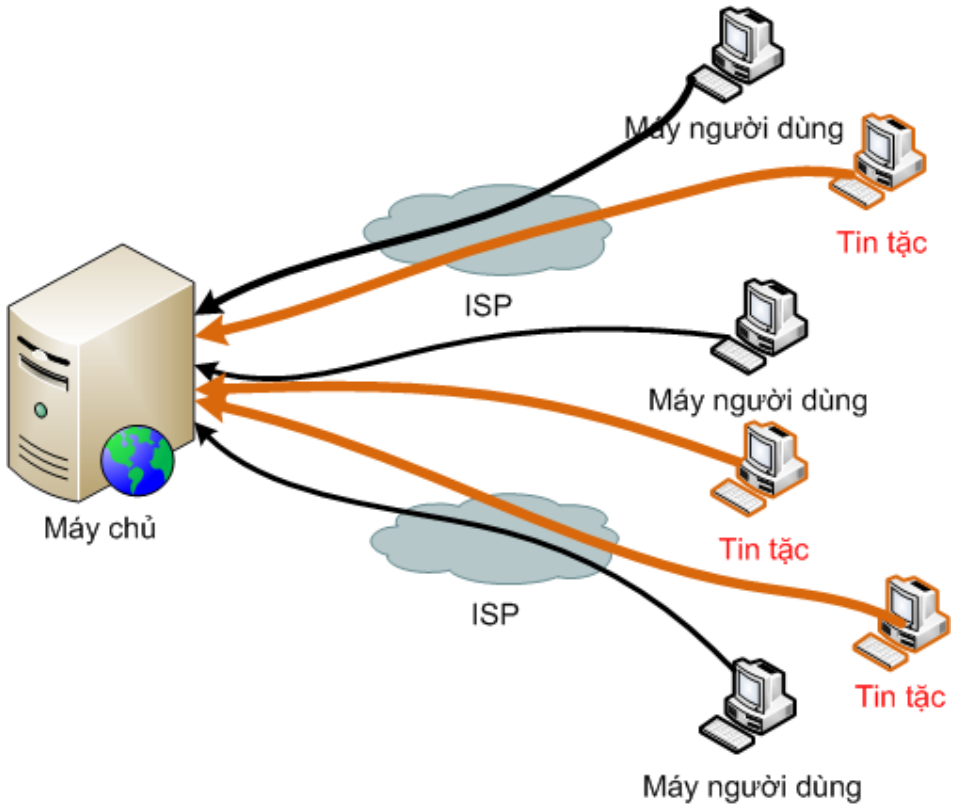


Hình 1.1 Mô hình kết nối mạng toàn cầu

Khi nhu cầu sử dụng của người tăng, lưu lượng các ứng dụng sẽ phát sinh nhiều làm cạn kiệt tài nguyên có giới hạn của hệ thống. Hệ thống mạng luôn luôn phát triển không ngừng và ngày càng được mở rộng đòi hỏi cần mức phí đầu tư về trang thiết bị cũng như cơ sở hạ tầng phù hợp. Tài nguyên trong hệ thống là do người quản lý phân phối, có thể điều chỉnh tùy theo nhu cầu người dùng theo thời gian. Với mức tài nguyên có hạn chế thì vấn đề cần thiết là phải đánh giá được tình trạng hoạt động của hệ toàn bộ thống để tránh trường hợp lãng phí khi đầu tư cơ sở

hạ tầng, nâng cấp trang thiết bị hay hệ thống bị quá tải dẫn đến chất lượng dịch vụ trong hệ thống bị suy giảm, ảnh hưởng đến người dùng.

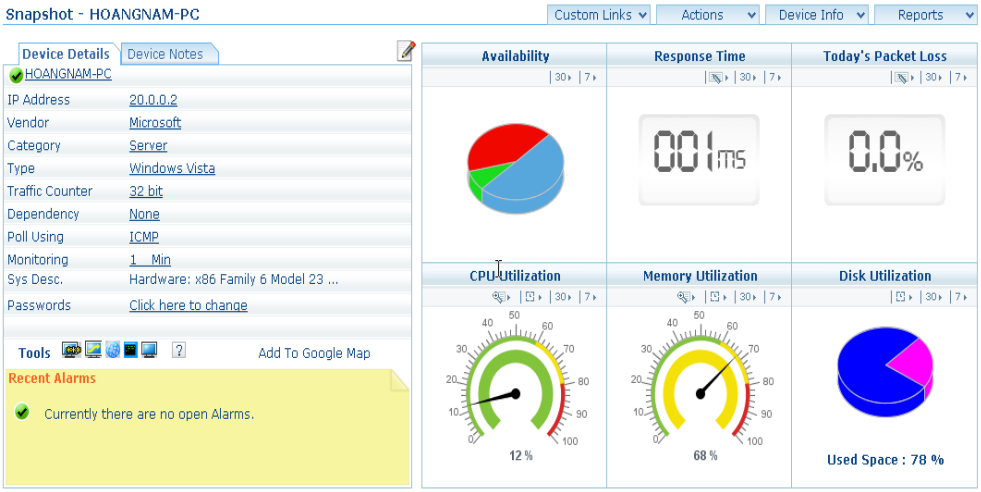
Vấn đề an ninh mạng cũng rất quan trọng trong thời buổi hiện nay. Với sự phát triển mạnh mẽ của mạng máy tính đã mang lại rất nhiều tiện ích cho người dùng. Tuy nhiên, tồn tại song song là các mối nguy hiểm từ tin tặc. Người quản trị mạng luôn phải đối đầu trong tư thế bị động trước các mối đe dọa này. Họ không biết trước được thời điểm cũng như phương thức tấn công nên thường sẽ không phản ứng kịp thời, dẫn đến hệ thống bị đình trệ, ảnh hưởng đến các dịch vụ và người dùng không truy cập được. Một trong các hình thức tấn công phổ biến nhất hiện nay là tấn công từ chối dịch vụ (DoS) vào các trang web. Loại hình tấn công này rất đa dạng, gây ra thiệt hại, mất mát lớn và thuộc loại khó bị phát hiện nên đã trở thành vũ khí lợi hại của tin tặc [1].



Hình 1.2 Tấn công từ chối dịch vụ đến máy chủ

Hình thức tấn công "flood" với số lượng lớn các yêu câu được sinh ra sẽ làm cho hệ thống bị chậm lại hay có thể gây ra gián đoạn. Không giống như kiểu tấn công phá hoại bằng virus, DDoS sử dụng số lượng lớn máy tính (có thể lên đến hàng triệu máy…) gởi các thông điệp HTTP GET gây ngập lụt hệ thống và việc phân tích dựa vào các công cụ quản trị mạng cũng trở nên khó khăn. Trong tất cả các loại tấn công DDoS, có hơn 90% sử dụng kỹ thuật khai thác trên nền tảng giao thức vận chuyển TCP. Hình thức tấn công phổ biến và hiệu quả là dựa vào cơ chế bắt tay ba bước của giao thức TCP. Với hình thức này, việc thiết lập kết nối sẽ không trọn vẹn, nhưng máy chủ lại phải duy trì bán kết nối này gây ra tổn hao tài nguyên [3]. Khi nhận được gói SYN, máy chủ sẽ hồi đáp lại bằng gói SYN/ACK ở cổng dịch vụ tương ứng. Cho đến khi máy chủ nhận được gói SYN/ACK từ máy khách thì nó vẫn phải duy trì bán kết nối này (half-open) trong khoảng thời gian chờ 75 giây. Máy chủ lưu lại các bán kết nối trong bộ nhớ cho đến khi đầy thì sẽ ngắt các bán kết nối này [4].

Để khai thác tài nguyên một cách hiệu quả và bảo vệ hệ thống mạng trước những nguy cơ khó lường trước cần phải có một hệ thống đánh giá, giám sát hiệu suất tài nguyên chính xác, đáng tin cậy. Khi đó, việc đánh giá hiệu suất hệ thống sẽ cho biết được nhu cầu sử dụng của máy chủ, thiết bị mạng, tình trạng bảo mật… để có được những giải pháp giải quyết nhu cầu sử dụng đúng cách, hiệu quả hơn, an toàn hơn và phù hợp với mức chi phí đầu tư.



Hình 1.3 Quản lý hiệu suất hệ thống với công cụ Opmanager

Vì vậy, giải pháp giám sát để có thông tin tổng quan về hệ thống một cách chính xác là điều cần thiết. Một công cụ có tính năng cảnh báo tấn công ngay khi phát hiện ra dấu hiệu và cảnh báo kịp thời cho người quản trị hệ thống. Với tính năng này sẽ giúp cho người quản trị viên chủ động hơn trong công tác bảo vệ hệ thống mạng, chuẩn bị được các phương án phòng chống phù hợp nhằm nâng cao khả năng cung cấp dịch vụ đến người dùng.

1.2 Hướng giải quyết

Giám sát hệ thống mạng luôn là yếu tố cần thiết và quan trọng hiện nay trong vấn đề an toàn hệ thống. Để đảm bảo được hệ thống an toàn là điều khó khăn, trong khi đó hệ thống mạng ngày càng được mở rộng nhằm đáp ứng cho số lượng người dùng ngày càng tăng, nguy cơ bị tấn công càng tăng cao. Do đó, việc duy trì chất lượng dịch vụ cao cho người sử dụng, quản trị viên phải đảm bảo nhiều tiêu chí như: không có tắt nghẽn trong mạng, nếu có tắt nghẽn thì phải loại bỏ càng sớm càng tốt. Tình trạng hoạt động của các thiết bị, nếu bị quá tải thì phải can thiệp để tránh hư hao. Tình trạng bảo mật hệ thống, nếu có tấn công thì phải phát hiện kịp thời để có giải pháp phòng ngự phù hợp… Ngoài ra, khi có bất kỳ sự thay đổi nào từ người sử dụng đều bị cấm, điều này để duy trì độ tin cậy trong hệ thống. Tuy

nhiên, người quản trị viên không đủ thời gian để luôn theo dõi, quan sát tất cả các tiêu chí này trong hệ thống mạng. Vì vậy, một giải pháp giúp cho người quản trị đảm bảo tài nguyên, bảo mật và các dịch vụ mạng luôn ở trạng thái tốt là cần thiết. Từ đó, ghi nhận lại tất cả những thông tin trong từng khoảng thời gian và thông báo về các vấn đề xảy ra càng sớm càng tốt, vì nếu thông báo quá trễ thì vấn đề nghiêm trọng sẽ xảy ra trong hệ thống. Khi nhận được thông báo quản trị viên sẽ có những so sánh cần thiết để có hướng giải quyết tốt hơn trong tương lai.

Hiện nay có rất nhiều công cụ, phần mềm để giám sát hệ thống mạng. Việc phải chọn một công cụ phù hợp để sử dụng và cài đặt trên một máy chủ dùng để quan sát và lưu trữ thông tin của những máy chủ và thiết bị mạng khác là điều cần cân nhắc. Dựa vào các công cụ đắc lực này, việc quản trị mạng sẽ trở nên đơn giản hơn, ví dụ: chúng ta sẽ dễ dàng thiết lập ra những chính sách cho từng máy chủ, từng dịch vụ, từng thiết bị, người dùng …trên công cụ giám sát để cảnh báo theo từng cấp độ cho nhân viên quản trị. Khi đó, từ xa nhân viên quản trị có thể xem các cảnh báo và có những biện pháp để xử lý, khắc phục vấn đề cảnh báo của các thiết bị trong tương lai, như: thay thế các các tài nguyên như thế nào theo từng hiện trạng của nó, và biết được nhu cầu sử dụng của phần mềm trên máy chủ sẽ sử dụng với tài nguyên ra sao, các loại tấn công vào hệ thống và cách phòng chống tương ứng. Từ đó, người quản trị sẽ có những yêu cầu đề xuất cấu hình cần thiết cho máy chủ mà chạy phần mềm hay dịch vụ, các thiết bị bảo mật cần thiết.

Đề tài này sử dụng công cụ Nagios, một công cụ mã nguồn mở, một ứng dụng rất mạnh cho việc giám sát hệ thống mạng. Nó phù hợp với các hệ thống mạng lớn và nhỏ. Ưu điểm lớn nhất của Nagios là tính mở của chương trình, ta có thể sử dụng Nagios theo nhiều cách, đồng thời có thể mở rộng tính năng theo nhu cầu của người sử dụng bằng cách phát triển các plugin. Đề tài này sẽ xây dựng tính năng cảnh báo tấn công để tích hợp vào trong công cụ Nagios giúp cho việc phát hiện, cảnh báo kịp thời khi hệ thống xuất hiện các dấu hiệu tấn công. Nhờ vào tính năng này sẽ giúp cho việc giải quyết vấn đề xảy ra trong hệ thống được tiến hành một cách hiệu quả nhất.

Mục đích Nagios là theo dõi toàn bộ cơ sở hạ tầng công nghệ thông tin để đảm bảo hệ thống, ứng dụng, bảo mật, dịch vụ và quy trình đang hoạt động tốt. Trong trường hợp có các dấu hiệu bất thường xảy ra, Nagios sẽ gửi cảnh báo vấn đề với quản trị viên, cho phép họ bắt đầu quá trình phục hồi trước khi bị sự cố, ảnh hưởng đến quá trình hoạt động, người sử dụng. Công cụ Nagios giúp xác định sự cố xảy ra đối với cơ sở hạ tầng quan trọng của hệ thống mạng một cách chính xác.

1.3 Ý nghĩa khoa học và thực tiễn

Nguy cơ bị tấn công trong mạng máy tính là mối lo ngại lớn, người quản trị mạng luôn trong tình huống bị động nên khó có được giải pháp phòng chống tốt trước các kiểu tấn công biến hóa liên tục. Như vậy, việc xây dựng thêm tính năng cảnh báo tấn công mới trên công cụ mã nguồn mở Nagios, nhằm phát hiện và cảnh báo kịp thời những nguy cơ trong vấn đề bảo mật hệ thống là cần thiết. Nhờ vào công cụ mã nguồn mở sẽ giúp tiết kiệm chi phí, giúp cho khả năng đáp ứng dịch vụ của hệ thống đến người dùng được nâng cao, người quản trị mạng chủ động hơn trước các tình huống xấu không mong muốn có thể xảy ra.

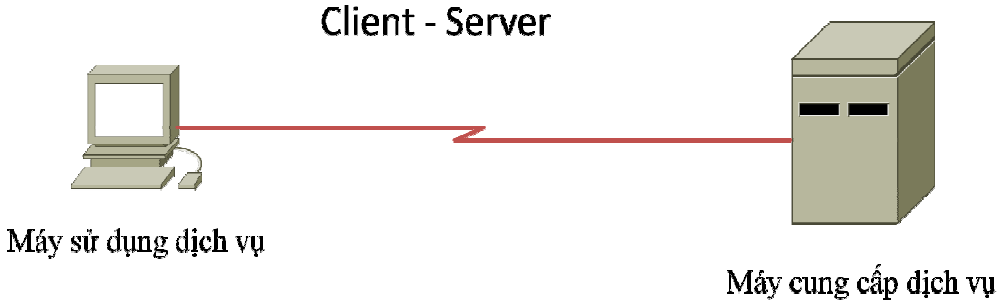
Các phương pháp tấn công phổ biến hiện nay thường khai thác cơ chế hoạt động của giao thức TCP. Đây là giao thức hướng kết nối với tính năng tin cậy, có cơ chế kiểm soát lỗi, kiểm soát luồng và kiểm soát tắc nghẽn. Trong quá trình giao tiếp, truyền thông bằng giao thức TCP, các máy tính sẽ trải qua ba quá trình. Đầu tiên là quá trình thiết lập kết nối qua ba bước bắt tay. Kế đến là quá trình truyền dữ liệu với các cơ chế kiểm soát lỗi, kiểm soát luồng và kiểm soát tắc nghẽn giúp cho giao thức TCP trở nên tin cậy hơn. Cuối cùng là quá trình ngắt kết nối để giải phóng tài nguyên cho máy chủ. Phương pháp nghiên cứu được sử dụng trong luận văn này tập trung vào quá trình đầu tiên, quá trình thiết lập kết nối của giao thức TCP. Tại giai đoạn này, thu thập các thông điệp được phát sinh một cách bất thường mà các phương pháp tấn công sử dụng để gây nguy hại cho máy chủ. Thống kê các thông điệp này và so sánh với ngưỡng an toàn được thiết lập trước. Từ kết quả này, đưa ra cảnh báo cho người quản trị viên về tình trạng an toàn của máy chủ.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1 Mô hình mạng phổ biến

2.1.1 Mô hình máy chủ - máy khách

Đây là mô hình phổ biến nhất trong mạng máy tính, máy chủ là máy có chức năng cung cấp dịch vụ cho các máy tính khác truy cập. Ngược lại, máy khách là máy truy cập, sử dụng các dịch vụ do máy tính khác cung cấp. Trong mô hình này, máy chủ luôn ở trạng thái chờ tiếp nhận yêu cầu dịch vụ từ máy khách. Trên thực tế, các máy chủ có thể liên kết lại với nhau nhằm tăng cường khả năng cung cấp dịch vụ cho số lượng lớn máy khách truy cập. Ưu điểm của mô hình này chính là các máy có thể làm việc với nhau trên bất kỳ nền tảng nào dựa vào chuẩn giao tiếp TCP/IP, mọi người có thể truy cập dịch vụ ở mọi nơi. Tuy nhiên với mô hình quản lý tập trung này, sức mạnh của hệ thống chính là ở máy chủ. Khi máy chủ gặp sự cố sẽ ảnh hưởng đến dịch vụ mà nó cung cấp. Bên cạnh đó, vấn đề an toàn thông tin, an minh mạng cũng là vấn đề lớn cần sự quan tâm đặc biệt.

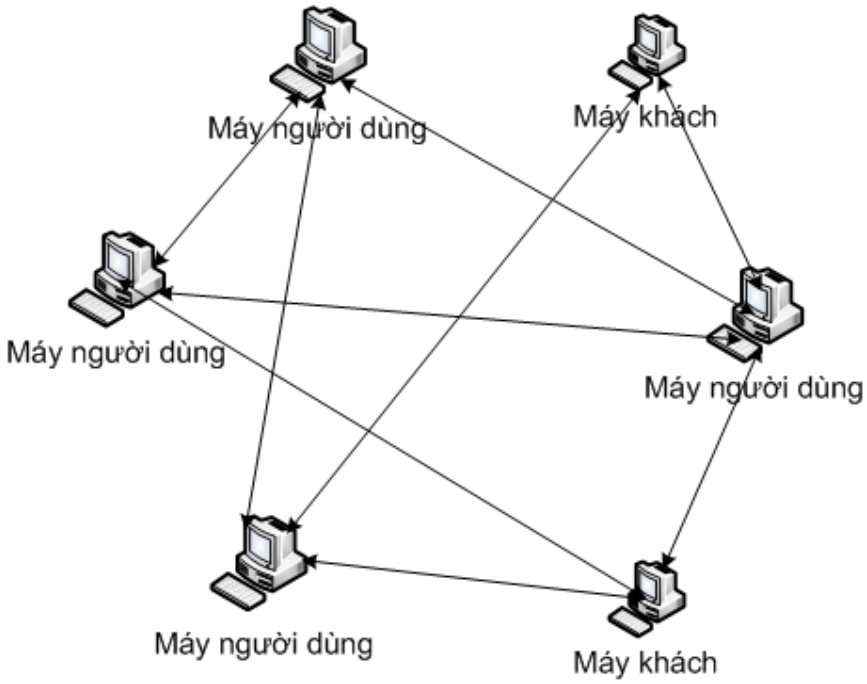


Hình 2.1 Mô hình mạng máy chủ - máy khách

2.1.2 Mô hình mạng ngang hàng (peer - to –peer)

Khác với mô hình máy chủ - máy khách, mạng ngang hàng không có máy chủ trung tâm và khai thác được sức mạnh của từng máy tham gia vào mạng, nếu số lượng máy tham gia vào mạng ngày càng tăng thì khả năng đáp ứng dịch vụ của cả hệ thống ngày càng lớn. Mỗi máy đều có chức năng vừa là máy chủ, vừa là máy

khách sẽ đóng góp vào khả năng lưu trữ, tính toán và tăng đường truyền…Tính chất phân tán của mạng cũng giúp cho mạng hoạt động tốt ngay khi có sự cố xảy ra.



Hình 2.2 Mô hình mạng ngang hàng

Trong cả hai mô hình trên, máy chủ luôn trong tình trạng chờ tiếp nhận các yêu cầu cung cấp dịch vụ từ máy khách. Khả năng đáp ứng dịch vụ của máy chủ được xác định dựa trên cấu hình phần cứng, các thông số mạng (băng thông, tốc độ truyền, độ trễ…). Các máy khách khi muốn sử dụng dịch vụ của máy chủ đều phải chủ động gửi các thông điệp dùng thiết lập kết nối đến máy chủ. Việc tiếp nhận các yêu cầu cung cấp dịch vụ từ máy khách với số lượng, tần suất lớn sẽ ảnh hưởng đến hiệu suất của máy chủ.

2.2 Bộ giao thức TCP/IP

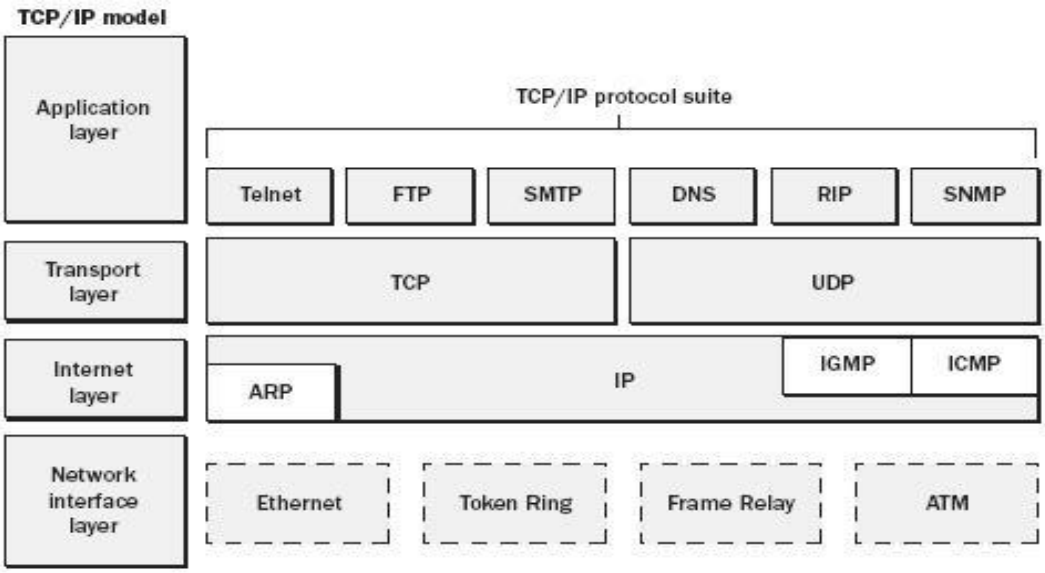
Đây là chuẩn chung được các máy tính sử dụng để giao tiếp với nhau. Cấu trúc bộ giao thức này bao gồm các lớp như sau:

- ✓ Lớp ứng dụng
- ✓ Lớp giao vận

- ✓ Lớp liên mạng
- ✓ Lớp giao diện vật lý

Trong đó, tầng giao vận cung cấp hai phương thức thiết lập phiên truyền thông giữa các máy tính là TCP và UDP.

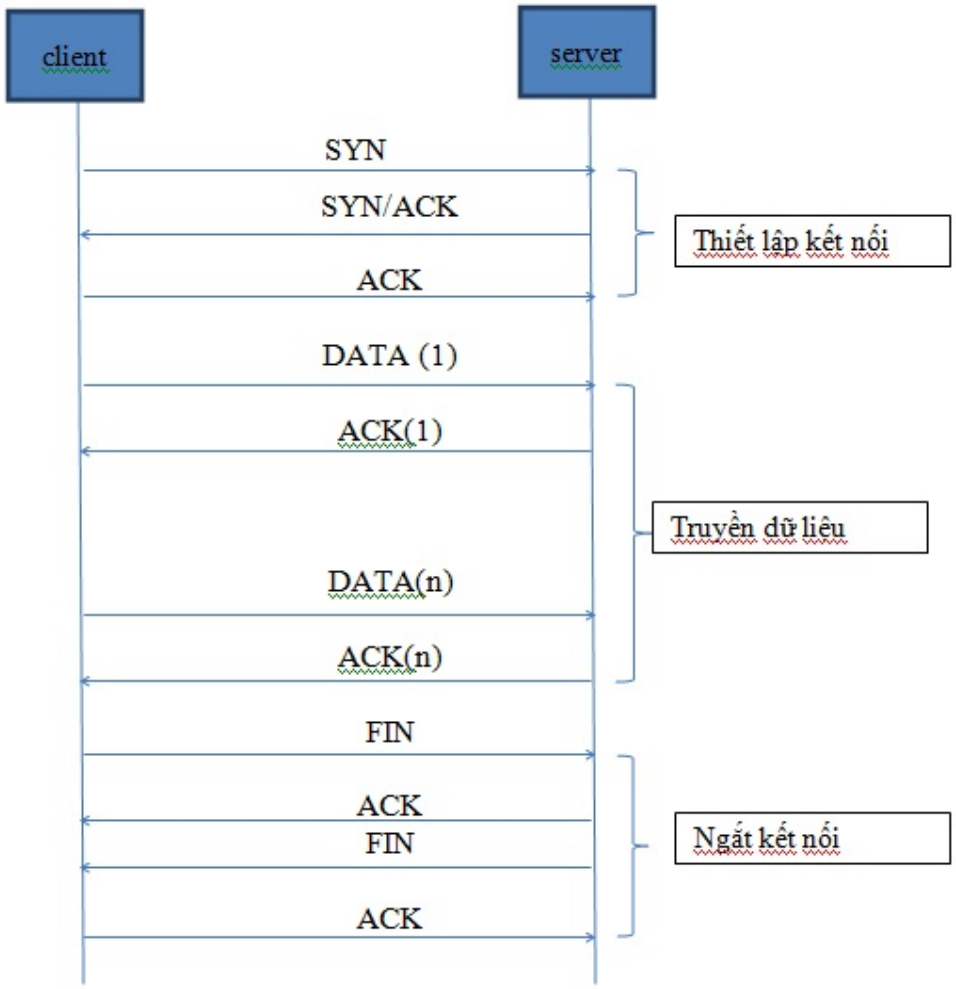
- UDP (User Datagram Prorocol): cung cấp phương thức truyền thông phi kết nối, không có cơ chế đảm bảo toàn vẹn dữ liệu. Các ứng dụng trên nền UDP thường có kích thước gói tin nhỏ, độ tin cậy phụ thuộc vào lớp ứng dụng.
- TCP (Transmission Control Protocol): Cung cấp kênh truyền thông hướng kết nối và đảm bảo toàn vẹn dữ liệu, độ tin cậy cao. Các ứng dụng trên nền TCP thường có kích thước gói tin lớn và yêu cầu xác nhận của bên nhận dữ liệu.



Hình 2.3 Kiến trúc bộ giao thức TCP/IP

2.3 Nguyên lý hoạt động của truyền thông hướng kết nối

Nguyên lý này quy định quy trình giao tiếp giữa các máy tính với nhau trong môi trường mạng dựa vào bộ giao thức TCP/IP, đặc biệt là giữa máy khách và máy chủ thông qua "ba bước bắt tay". Để khởi tạo kênh kết nối, máy khách gửi thông điệp đồng bộ đến máy chủ (SYN) nhằm yêu cầu thiết lập kết nối. Sau đó, máy chủ sẽ phản hồi lại thông điệp (SYN/ACK) nếu như có khả năng đáp ứng yêu cầu cho máy khách. Sau đó, máy khách phản hồi lại bằng thông điệp ACK. Sau thông điệp này, kết nối giữa hai máy được thiết lập.



Hình 2.4 Quá trình giao tiếp của máy tính bằng TCP

Do TCP có độ tin cậy cao, đảm bảo toàn vẹn dữ liệu trong quá trình giao tiếp, nên cơ chế này thường được sử dụng trong các ứng dụng quan trọng, không cho phép mất dữ liệu khi giao tiếp trong môi trường mạng. Máy nhận khi nhận được gói dữ liệu sẽ dùng thông điệp ACK để phản hồi lại cho máy gửi nhằm thông báo việc nhận dữ liệu thành công và yêu cầu khối dữ liệu tiếp theo. Trong trường hợp không nhận được dữ liệu (máy nhận không phản hồi ACK), máy gửi sẽ gửi lại gói dữ liệu bị mất trước đó sau khi hết thời gian chờ (RTO - Retransmission Timeout).

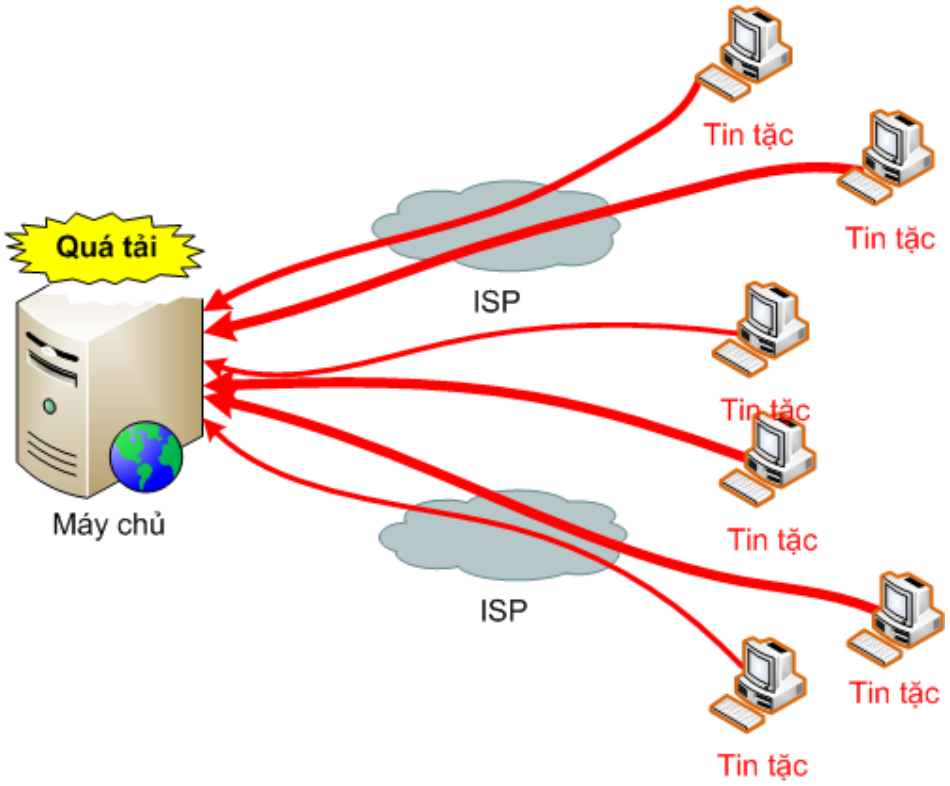
Khi gói dữ liệu cuối cùng được gửi đi, máy gửi sẽ báo ngắt kết nối bằng thông điệp FIN và nhận phản hồi ACk từ máy nhận. Khi đó, nếu máy nhận đã nhận đầy đủ các gói dữ liệu sẽ gửi lại thông điệp FIN và chờ nhận phản hồi lại bằng thông điệp ACK để chấm dứt quá trình giao tiếp. Lúc này, kết nối giữa hai máy sẽ bị ngắt.

2.4 Vấn đề an ninh mạng

Đây là vấn đề lâu nay vẫn gây lo ngại cho các cấp quản lý cũng như đông đảo người dùng và giới doanh nghiệp, đó là các cuộc xâm nhập mạng trái phép ngày càng gia tăng đáng kể. Hiện nay, xu hướng có thể nhận thấy là sự thay đổi các dạng tấn công trên mạng, với độ phức tạp ngày càng tăng. Hệ thống an ninh mạng trước đây có thể là đủ để bảo vệ các doanh nghiệp thì nay cũng không còn đảm bảo nữa. Động cơ của tin tặc cũng khác trước. Trước đây, tin tặc có thể tấn công một website, để lại lời nhắn trên website nhằm chứng minh với cộng đồng khả năng tấn công của hackers, để giành được sự nổi tiếng. Những cuộc tấn công đó thường ầm ĩ, một virus phát tán ra cả thế giới đều biết và rất nhiều nơi bị ảnh hưởng. Nhưng giờ đây, bản chất các cuộc tấn công hoàn toàn khác. Động cơ tài chính được đặt lên hàng đầu. Trước các mối nguy hiểm đó, giải pháp bảo vệ thụ động (reactive): chỉ phản ứng sau khi tấn công xảy ra, đã không còn hiệu quả, cần bảo vệ một cách chủ động (proactive) chống lại những cuộc tấn công mạng. Vấn đề cần thiết là phát hiện kịp thời các dấu hiệu tấn công để có thể áp dụng các phương pháp phòng chống chủ động hiệu quả hay khắc phục sự cố trong thời gian nhanh nhất.

2.5 Tấn công từ chối dịch vụ

Đây là một trong các phương pháp tấn công phổ biến và được giới tin tặc sử dụng thường xuyên. Trong tất cả các loại hình tấn công, thì đây là phương pháp đáng lo ngại vì sau mỗi cuộc tấn công, hậu quả để lại là khá nghiêm trọng. Có rất nhiều kỹ thuật tấn công trong phương pháp này và thường xuyên kết hợp với nhau, biến hóa đa dạng. Điều này gây khó khăn trong việc phát hiện ra dấu hiệu của mỗi đợt tấn công. Người quản trị hệ thống không biết trước được các mối hiểm họa và luôn trong trạng thái bị động nên không có được biện pháp phòng chống thích hợp.



Hình 2.5 Tấn công từ chối cung cấp dịch vụ đến máy chủ

2.5.1 Tấn công SYN

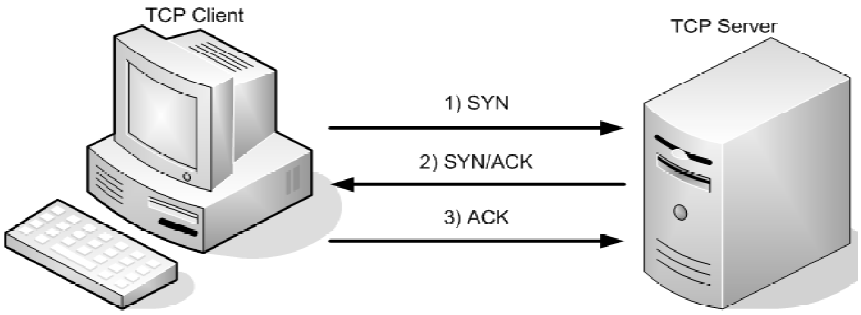
Được là một trong những kiểu tấn công DoS kinh điển nhất. Kiểu tấn công này dựa trên nguyên lý thiết lập kết nối của TCP thông qua "bắt tay ba bước", mỗi

khi máy khách muốn thực hiện kết nối với máy chủ thì sẽ thực hiện quá trình bắt tay ba bước thông qua các gói tin.

- Bước 1: Máy khách sẽ gửi các gói tin (chứa SYN=1) đến máy chủ để yêu cầu kết nối thiết lập kết nối.

- Bước 2: Khi nhận được gói tin SYN, máy chủ sẽ gửi lại gói tin SYN/ACK để thông báo cho máy khách biết là đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Máy chủ sẽ giành một phần tài nguyên hệ thống như bộ nhớ đệm để nhận và truyền dữ liệu. Ngoài ra, các thông tin khác của máy khách như địa chỉ IP và cổng cũng được ghi nhận.

- Bước 3: Cuối cùng, máy khách hoàn tất việc bắt tay ba bước bằng cách hồi âm lại gói tin chứa ACK cho máy chủ và tiến hành truyền dữ liệu.

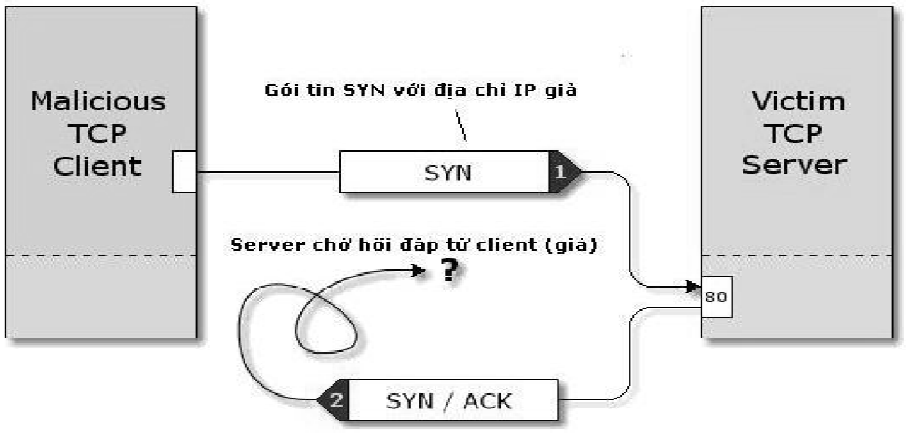


Hình 2.6 Quá trình thiết lập kết nối

TCP là giao thức tin cậy trong việc giao nhận nên trong lần bắt tay thứ hai, máy chủ gửi các gói tin SYN/ACK trả lời lại máy khách mà không nhận lại được hồi âm của máy khách để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lập lại việc gửi gói tin SYN/ACK cho máy khách đến khi nào nhận được hồi đáp của máy máy khách.

Các phương pháp tấn công dạng này sẽ làm cho máy khách không hồi đáp thong điệp ACK cho máy chủ, trong khi máy chủ vẫn tiếp tục lặp lại việc gửi gói tin SYN/ACK và giành tài nguyên để chờ thiết lập kết nối. Trong lúc tài nguyên của hệ thống có giới hạn, tin tặc sẽ tìm cách gia tăng số lượng máy tham gia vào quá trình

này để chiếm giữ phần lớn tài nguyên của máy chủ. Phương pháp tấn công này sẽ gây giảm hiệu suất của máy chủ một cách nhanh chóng.



Hình 2.7 Tấn công giả địa chỉ IP

Nếu quá trình đó kéo dài, máy chủ sẽ nhanh chóng trở nên quá tải, dẫn đến tình trạng treo nên các yêu cầu hợp lệ sẽ bị từ chối không thể đáp ứng được. Có thể hình dung, quá trình này cũng giống như khi máy tính bị treo khi mở cùng lúc quá nhiều chương trình cùng lúc.

Nếu tin tặc tiếp tục gửi nhiều gói tin SYN đến máy chủ thì cuối cùng máy chủ cũng không thể tiếp nhận thêm kết nối nào nữa, dù đó là các yêu cầu kết nối hợp lệ. Việc này đồng nghĩa với việc máy chủ không tồn tại và xảy ra nhiều tổn thất do ngưng trệ hoạt động, đặc biệt là trong các giao dịch thương mại điện tử trực tuyến.

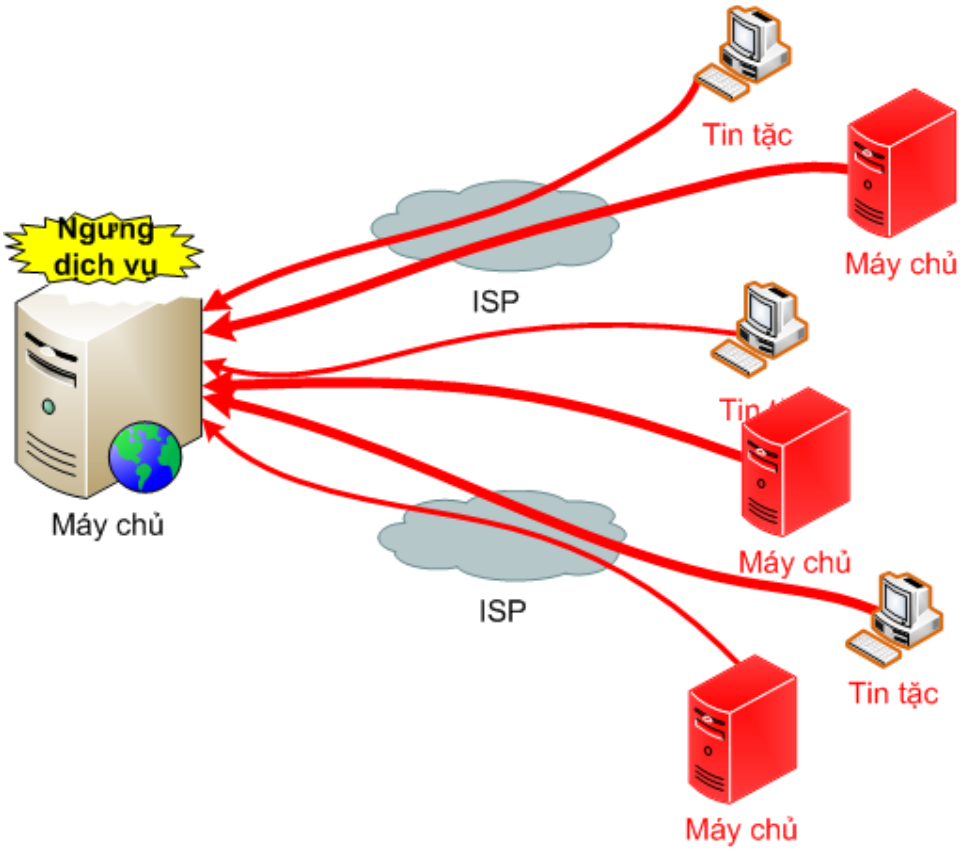
2.5.2 Tấn công Flood

Một kiểu tấn công DoS nữa cũng rất hay được dùng vì tính đơn giản và vì có rất nhiều công cụ sẵn có hỗ trợ rất nhiều cho kẻ tấn công là Flood Attack, chủ yếu thông qua các website.

Về nguyên tắc, các website đặt trên máy chủ khi chạy sẽ chiếm lượng tài nguyên máy chủ nhất định, nhất là lượng bộ nhớ (RAM) và bộ vi xử lý (CPU). Dựa vào việc tiêu hao đó, kẻ tấn công dùng các phần mềm (ví dụ như smurf) để liên tục yêu cầu máy chủ phục vụ trang web đó để chiếm dụng tài nguyên. Cách tấn công này tuy không làm máy chủ ngừng cung cấp dịch vụ hoàn toàn nhưng sẽ làm cho tốc độ phục vụ của toàn bộ hệ thống giảm mạnh, người dùng sẽ cảm nhận rõ ràng việc phải chờ lâu hơn để trang web hiện ra trên màn hình. Nếu thực hiện tấn công ồ ạt và có sự phối hợp nhịp nhàng, phương thức tấn công này hoàn toàn có thể làm tê liệt máy chủ trong một thời gian dài.

2.5.3 Tấn công từ chối dịch vụ phân tán (DDoS)

Kỹ thuật này dựa trên nguyên lý tấn công DoS cổ điển, sức mạnh của DDoS mạnh hơn rất nhiều lần nhờ vào số lượng lớn máy tính tham gia vào mỗi đợt tấn công. Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống dẫn đến hệ thống ngưng hoạt động. Để thực hiện thì người tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính hay mạng máy tính trung gian (mạng zombie) từ nhiều nơi để đồng loạt gửi ào ạt các gói tin với số lượng rất lớn nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó.



Hình 2.8 Tấn công ngưng cung cấp dịch vụ của máy chủ

Theo cách này, hệ thống có đường truyền tốc độ cao cũng không thể chịu đựng được số lượng hàng triệu các gói tin gửi đến và dẫn đến hệ thống không thể hoạt động được nữa. Khi các yêu cầu hợp lệ khác được gửi đến tại thời điểm diễn ra tấn công sẽ không thể nào được đáp ứng.

2.5.4 Tấn công từ chối dịch vụ phản xạ nhiều vùng DRDoS

Đây là kiểu tấn công khá mới và mạnh trong kiểu tấn công DoS, bằng cách sử dụng kỹ thuật này có thể hạ gục bất cứ hệ thống nào trong khoảng thời gian ngắn. Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy chủ, làm tắc nghẽn hoàn toàn đường kết nối từ máy chủ vào mạng Internet và làm tiêu hao tài nguyên máy chủ. Trong suốt quá trình máy chủ bị tấn công bằng DRDoS,

máy khách không thể kết nối được vào máy chủ để truy cập dịch vụ. Tất cả các dịch vụ chạy trên nền TCP/IP như DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa.

DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS. Với kiểu tấn công SYN với một máy tính đơn, vừa có sự kết hợp giữa nhiều máy tính để chiếm dụng băng thông như kiểu DDoS. Kẻ tấn công giả mạo địa chỉ của máy chủ mục tiêu rồi gửi yêu cầu SYN đến các máy chủ khác để các máy chủ này gửi các gói tin SYN/ACK đến máy chủ mục tiêu. Các máy chủ lớn, đường truyền mạnh đó đã vô tình tham gia vai trò trung gian cho kẻ tấn công như trong DDoS. Quá trình gửi cứ lặp lại liên tục với nhiều địa chỉ IP giả từ kẻ tấn công, với nhiều máy chủ lớn tham gia nên máy chủ mục tiêu nhanh chóng bị quá tải, băng thông bị chiếm dụng bởi máy chủ lớn.

2.6 Phương pháp phòng chống tấn công từ chối dịch vụ

Các kỹ thuật sử dụng trong tấn công từ chối dịch vụ khá đơn giản, nhưng rất khó phòng chống do tính bất ngờ và thường là phòng chống trong thế bị động khi sự việc đã xảy ra. Việc đối phó bằng cách nâng cấp hệ thống (phần cứng, đường truyền và phần mềm…) là giải pháp tốt nhưng với chi phí khá cao. Biện pháp tối ưu là phải thường xuyên theo dõi, giám sát để phát hiện và ngăn chặn kịp thời các dấu hiệu tấn công ngay từ ban đầu để áp dụng các biện pháp phòng chống hiệu quả hơn. Một số biện pháp cơ bản để khắc phục khi xuất hiện tấn công được đề suất như sau:

- ✓ Truy tìm địa chỉ IP đó và cấm không cho gửi dữ liệu đến máy chủ.
- ✓ Dùng tính năng lọc dữ liệu của router/firewall để loại bỏ các gói tin không mong muốn, giảm lượng lưu thông trên mạng và tải của máy chủ.
- ✓ Đặt lại giới hạn trên router/firewall để hạn chế số lượng gói tin vào hệ thống.
- ✓ Cập nhật các bản sửa lỗi cho hệ thống đó hoặc thay thế.
- ✓ Dùng một số cơ chế, công cụ, phần mềm để chống lại TCP SYN Flooding.

- ✓ Tắt các dịch vụ khác không cần thiết (nếu có) trên máy chủ để giảm tải và có thể đáp ứng tốt hơn. Có thể nâng cấp các thiết bị phần cứng để nâng cao khả năng đáp ứng của hệ thống hay sử dụng thêm các máy chủ cùng tính năng khác để phân chia tải.
- ✓ Tạm thời chuyển máy chủ sang một địa chỉ khác.

2.7 Phương pháp dò tìm, phát hiện các dấu hiệu tấn công từ chối dịch vụ

Để có thể áp dụng các biện pháp phòng chống tấn công hiệu quả, thì việc quan trong là phát hiện càng sớm càng tốt các dấu hiệu tấn công được áp dụng. Ngày nay, có nhiều phương pháp dò tìm tấn công từ chối dịch vụ với mục đích phát hiện, tính toán và ngăn chặn kịp thời. Có nhiều nhà nghiên cứu, nhóm nghiên cứu đã đề xuất nhiều phương pháp dò tìm, phát hiện tấn công SYN hiệu quả. Theo [1], tác giả đã đề suất phương pháp dò tìm tấn công DDoS và ngăn chặn trên kiến trúc đám mây tại các bộ định tuyến biên. Phương pháp này có đặc tính tương thích cao và đáng tin cậy, không chứa đựng các gói bổ sung và chất lương dịch vụ tốt. Trong thuật toán này, sẽ loại bỏ các luồng tấn công nếu phát hiện, ngược lại là các luồng hợp lệ và sẽ được chuyển tiếp đến đích. Trong [2],[8] đề cập đến phương thức dò tìm tấn công DDoS vào giao thức ở lớp ứng dụng web, với phương thức GET của HTTP. Phương thức sử dụng để dò tìm là thuật toán dựa trên số lượt truy cập và thuật toán truy cập mẫu và ứng dụng trong ngành công nghiệp lưu trữ với dữ liệu phát sinh rất lớn. Một phương pháp đơn giản so với các phương pháp khác được đề suất để dò tìm tấn công bằng cách sử dụng thuật toán tính tổng tích lũy phi tham số [3] và có kết quả khá tốt để phát hiện ra khi có dấu hiệu tấn công TCP-SYN.

Một phương pháp khác được đề suất dựa vào cặp thông điệp TCP SYN-FIN trên nền tảng TCP và sử dụng thuật toán tính tổng tích lũy (CUSUM)[4],[9]. Đặc điểm của phương pháp này là dễ dàng triển khai, có hiệu quả cao và tìm ra được nguồn tấn công. Phương pháp này so sánh số lượng gói SYN và FIN, nếu tỉ lệ gói

SYN cao hơn nhiều so với FIN theo thuật toán tích lũy phi tham số sẽ nhận diện ra tấn công. Tuy nhiên, phương pháp này chỉ áp dụng tại các bộ định tuyến biên [4].

Các phương pháp trên đều giải quyết vấn đề phát hiện các dấu hiệu của tấn công từ chối dịch vụ. Tuy nhiên, các thuật toán áp dụng khá phức tạp và triển khai khó khăn. Việc phân tích các dấu hiệu chưa đầy đủ dẫn đến kết quả chỉ tìm ra được các kỹ thuật tấn công giới hạn, sẽ có một số kỹ thuật tấn công không bị phát hiện. Điều cần thiết là có được thuật toán đơn giản, dễ dàng triển khai, cài đặt, được áp dụng trên nền tảng mã nguồn mở để có thể được sử dụng rộng rãi hơn mà vẫn đảm bảo được vấn đề hiệu quả và dễ dàng cho phép người dùng cập nhật các dấu hiệu mới. Việc tìm ra được một phương pháp chung, có thể phát hiện ra được hầu hết các dấu hiệu tấn công là điều khó khăn vì các phương pháp tấn công luôn biến hóa, nên cần một cơ chế linh hoạt cho người dùng có thể cập nhật thêm các dấu hiệu tấn công mới, cho phép tùy chỉnh các giá trị (ngưỡng) thích hợp với từng thông số mạng cụ thể.

CHƯƠNG 3: BÀI TOÁN VÀ GIẢI PHÁP

3.1 Hiện trạng

Trong hệ thống mạng thường có nhiều máy chủ và thiết bị mạng được sử dụng để phục vụ nhu cầu của người dùng truy cập từ bên trong cũng như từ bên ngoài hệ thống. Đặc biệt hơn là có những máy chủ cơ sở dữ liệu và ứng dụng để thực hiện các công việc trên. Ngoài các máy chủ được sử dụng phổ biến còn có các thiết bị mạng như switch, router, firewall làm nhiệm vụ tạo các kết nối giữa các thiết bị lại với nhau. Trong các thiết bị đó điều có sử dụng các dịch vụ như: HTTP, HTTPS, SSH,…; và còn có tài nguyên sử dụng như CPU, RAM, DISK,…

Bên cạnh việc đáp ứng nhu cầu của người dùng thì hệ thống mạng luôn đứng trước mối đe dọa không lường trước từ tin tặc. Hệ thống mạng luôn bị động trước các kỹ thuật tấn công tiên tiến, thời điểm tấn công không xác định và các máy tham gia tấn công với số lượng rất lớn, trong đó có các máy chủ trung gian mạnh. Tại thời điểm bị tấn công, dịch vụ mạng có dấu hiệu bị đình trệ, người dùng truy cập khó khăn… Các phương thức tấn công luôn thay đổi gây khó khăn trong việc phát hiện kịp thời và đề ra phương pháp phòng chống hợp lý dẫn đến sự suy giảm khả năng đáp ứng của hệ thống.

3.2 Vấn đề

Bất cứ khi nào một vấn đề phát sinh trong quá trình đang cung cấp dịch vụ, hoặc là trong hệ thống hạ tầng mạng, thì việc tìm ra nguồn gốc vấn đề thường là rất lâu. Phần mềm quản lý tiến trình quan sát các tiến trình, nhưng không quan sát các thành phần hỗ trợ, chẳng hạn như phần cứng máy chủ, các thành phần mạng, các kết nối mạng. Ví dụ, khi một máy chủ chạy dịch vụ web bị dừng kết nối, kết quả là ở trong các tiến trình cung cấp dịch vụ bị hư hỏng, nhưng lại hiển thị không rõ ràng. Hơn nữa, nhân viên quản trị không có thông tin để xác định điều gì đã xảy ra sai. Nhân viên quản trị phải kiểm tra bằng tay để đảm bảo tất cả hệ thống đều đang hoạt động. Quản trị viên không có thông tin tổng quan toàn bộ hệ thống tại cơ quan khi

mà gặp sự cố xảy ra. Điều này gây ra quá nhiều khó khăn để phát hiện lỗi gì đã xây ra.

Việc có quá ít thông tin có sẵn về phần cứng, bảo mật, mạng và hạ tầng, và quá nhiều hoặc quá khác biệt thông tin của các phần mềm trong mạng, để có thể giải quyết vấn đề một cách đầy đủ được. Điều này ảnh hưởng lớn đến công việc quản lý hệ thống.

Do nhu cầu phát triển hệ thống mạng theo thời gian, số lượng người dùng tăng thì vấn đề nâng cấp hệ thống là cần thiết: các thiết bị phần cứng cho máy chủ (RAM, CPU, HDD…), thiết bị mạng (switch, router, firewall…), đường truyền kết nối…. Hiện nay, vẫn chưa có một cơ sở để tính toán rõ ràng khi nâng cấp liệu có gây lãng phí (nâng cấp dư tài nguyên) hoặc thiếu hụt tài nguyên. Bên cạnh đó, hệ thống mạng luôn đứng trước các nguy cơ, mối đe dọa không lường trước của tin tặc. Các cuộc tấn công thường xuyên xảy ra và gây ra rất nhiều hậu quả xấu. Việc truy tìm ra đối tượng tấn công để xác định phòng ngừa, ngăn chặn là cả vấn đề nan giải. Phương pháp tấn công mà tin tặc sử dụng luôn thay đổi và biến hóa tinh vi gây khó khăn trong việc phát hiện để có biện pháp phòng ngừa thích hợp.

Với công cụ Nagios, các vấn đề liên quan trên đã được giải quyết bằng các module tính năng tích hợp sẵn. Các tính năng này giúp cho người quản trị có thông tin đầy đủ về cơ sỡ hạ tầng cũng như đánh giá hiệu suất của hệ thống. Tuy nhiên, vấn đề phát hiện ra các loại tấn công từ chối dịch vụ để nâng cao an toàn hệ thống thì chưa được giải quyết. Để có thể đối phó trước các cuộc tấn công có quy mô và đầy tính bất ngờ thì việc phát hiện ra sớm các dấu hiệu tấn công ngay tại thời điểm đầu tiên của cuộc tấn công sẽ mang lại thế chủ động cho người quản trị mạng. Từ đó sẽ giúp cho người quản trị viên có phương án phòng chống và khắc phục hợp lý để giảm thiểu thiệt hại cho hệ thống.

3.3 Mục tiêu và kết quả mong muốn đạt được của bài toán

Dựa trên công cụ giám sát hệ thống mã nguồn mở với các tính năng giám sát hiệu suất mạng sẵn có, để giải quyết bài toán trên bằng cách xây dựng một giải pháp

cho phép việc quản lý hoạt động được tổng quan và giám sát tình trạng của môi trường hệ thống máy chủ và hạ tầng mạng, bảo mật mạng. Giải pháp này phải cho phép tất cả các quản trị viên giám sát và xử lý nhanh chóng trong trường hợp có nhiều vấn đề xảy ra, đặc biệt là khi hệ thống bị tấn công.

Mục tiêu:

- Hạ tầng: theo dõi tình trạng an ninh của máy chủ

-Xây dựng tính năng phát hiện tấn công dịch vụ trên máy chủ: phát hiện tấn công kịp thời từ các dấu hiệu ban đầu của các kỹ thuật tấn công từ chối dịch vụ phổ biến.

Kết quả mong muốn:

- Thống kê số liệu ghi nhận tình trạng các máy chủ trên giao diện công cụ, và báo cáo kết quả thu được cho người quản lý cấp trên khi có yêu cầu.

- Thu thập số liệu đã thống kê để thấy rõ được những cuộc tấn công vào hệ thống. Phát hiện và cảnh báo kịp thời khi có dấu hiệu tấn công từ chối dịch vụ vào máy chủ.

- Gửi thông tin cảnh báo theo mức độ tức thì khi có sự thay đổi trạng thái hoạt động của hệ thống giám sát đến người quản lý phụ trách. Từ đó, người phụ trách sẽ biết vấn đề mà giải quyết ngay, giảm rủi ro ngưng thời gian hoạt động của hệ thống.

3.4 Công nghệ giám sát mạng SNMP

3.4.1 Định nghĩa

Giao thức Simple Network Management Protocol (SNMP) được thiết kế để một hệ thống giao tiếp với những thiết bị mạng có tác nhân SNMP agent. Tác nhân SNMP agent làm nhiệm vụ lấy thông tin về các thiết bị và gửi thông tin lấy được về hệ thống quản lý đạng lắng nghe trên địa chỉ mạng. Để cung cấp thông tin bảo mật, SNMP chỉ định sử dụng chuỗi giao tiếp gắn kèm với mỗi thông tin trên mạng. Nếu

một agent không nhận biết được chuỗi ký tự được người quản lý cấu hình thì sẽ không trả lời truy vấn.

SNMP hoạt động trên giao thức UDP. Một SNMP agent lắng nghe cổng 161 để SNMP lấy và SNMP gửi yêu cầu. Lấy yêu cầu thì sử dụng đọc thông tin và gửi yêu cầu để ghi giá trị. Trong SNMP phiên bản 1 và 2c thì thông tin trên mạng được chuyển ở dạng văn bản.

3.4.2 Cơ sở dữ liệu MIB

SNMP sử dụng cơ sở dữ liệu gọi là MIB để quản lý các loại thiết bị khác nhau trong mạng. MIB bao gồm các đối tượng được định nghĩa bằng cách sử dụng một bộ Abstract Syntax Notation One (ASN.1), được gọi là cấu trúc thông tin quản lý phiên bản 2 (SMIv2). Những đối tượng trong MIB đều thể hiên dạng số hay là chuỗi xác định đối tượng gọi là IOD. Ví dụ, số OID cho thời gian bắt đầu hoạt động của một hệ thống là 1.3.6.1.2.1.1.3 và có tên là sysUpTime.

Các MIB thường được các nhà sản xuất phần cứng cung cấp phù hợp với các thiết bị. Một OID luôn luôn là duy nhất, và mỗi nhà sản xuất thường có một MIB riêng của nó hoặc là những MIB chuẩn dùng chung được định nghĩa bởi Internet Engineering Task Force (IETF). Các MIB thường được cập nhật thường xuyên với những chức năng mới nhất, gỡ bỏ các chức năng quá cũ và sửa các lỗi ở phiên bản trước.

3.4.3 Các phiên bản

Giao thức SNMP có ba phiên bản riêng biệt: phiên bản 1 SNMPv1, phiên bản 2c SNMPv2c (hiểu như phiên bản 1.5) và phiên bản kế tiếp hiện nay là phiên bản 3 SNMPv3. Trong phiên bản 2c đã thay đổi và cải tiến hầu như bảo mật hơn phiên bản 1. Phiên bản mới có những cải tiến trong cách xử lý gói tin và hiệu xuất, những thực sự không có bất kỳ tính năng mới. Tuy nhiên phiên bản 3 giới thiệu các tính năng mới, mã hóa gói tin bảo vệ dữ liệu, toàn vẹn thông tin để đảm bảo dữ liệu không bị sửa đổi và xác thực để chứng minh nguồn dữ liệu an toàn.

Tính bảo mật trong phiên bản 3 được cải thiện bằng cách loại bỏ chuỗi giao tiếp và thay thế nó với một kiểu bảo mật người sử dụng (USM). Kiểu mới này có ba cấp bậc bảo mật riêng biệt: noAuthNoPriv, authNoPriv, và authPriv. Trong những cấp bảo mật này chúng ta có thể chọn một cách chứng thực và riêng tư nếu chúng ta muốn. Cấp bậc authPriv có hai yếu tố bắt buộc: riêng tư có nghĩa là mã hóa nội dụng và chứng thực. Được mã hóa trước khi gửi nó trên mạng bằng cách sử dụng chức năng mã hóa MD5 hoặc SHA1. Chuỗi mã hóa được tạo ra phải được gửi tới SNMP agent mà có chuỗi mã hòa giống với chuỗi đã được gửi. Nội dung thông tin được mã hóa bằng cách sử dụng giải thuật mã hóa DES với khóa riêng để mã hóa.

3.5 Giải pháp giám sát hệ thống Nagios

3.5.1 Lịch sử

Lịch sử của Nagios bắt đầu với Ethan Galstad, một nhà khoa học máy tính đã tốt nghiệp trường Minnesota của Mỹ, người đầu tiên đã sinh ra Nagios. Năm 1996 Galstad đã tạo ra chương trình MS-DOS đơn giản để sử dụng những phần mềm thứ 3 để kiểm tra sự tồn tại của các nút mạng từ xa và báo cáo kết quả như các trang số (được gọi là Ping). Ping nghĩa là gửi một gói tin “ICMP echo request” trên mạng đến máy nhận và nhận được gói tin trả lời “ICMP echo reply”. Hai năm sau, Galstad bắt đầu xây dựng nhiều ứng dụng phức tạp hơn để chạy trên hệ điều hành Linux. Xu hướng đó đã dẫn vào một dự án mã nguồn mỡ được gọi NetSaint, và sau đó được đổi tên là Nagios có lý do hợp lý. Từ viết tắt của Nagios là “Nagios Ain't Gonna Insist On Sainthood”.

3.5.2 Các đối tượng trong Nagios

Phần mềm Nagios quan sát những mục tiêu khác nhau được gọi là các đối tượng. Chúng được định nghĩa trong cấu hình như các dịch vụ (services), nhóm dịch vụ (service groups), các máy chủ (hosts), các nhóm máy chủ (host groups), các đầu mối liên lạc (contacts), nhóm liên hệ (contact groups), các lệnh (commands), các khoảng thời gian (time periods), những cấp bậc thông báo, những phụ thuộc thông

báo, những phụ thuộc thực thi. Các đối tượng không cần được định nghĩa như các dòng độc lập. Các mẫu đối tượng có thể được dùng khi định nghĩa các máy chủ chỉ định, và các thuộc tính được định nghĩa trong một mẫu sẽ được thừa kế của một đối tượng. Sự thừa kế cũng có thể được sử dụng để chia cấu hình thành những mẫu nhỏ hơn. Đối với những nhóm liên lạc, những đầu mối liên hệ đang chạy có thể được định nghĩa như những mục sở hữu của chúng, và sau đó được sử dụng cho một máy chủ chỉ định hoặc một dịch vụ.

3.5.3 Các kiểm tra của Nagios

Quan trọng hơn, Nagios xây dựng trên những kiểm tra về dịch vụ, kiểm tra máy chủ. Trong cấu hình một định nghĩa những đối tượng của máy chủ và những đối tượng về dịch vụ. Cơ bản một máy chủ được quan sát dựa vào một tên miền dịch vụ hoặc một địa chỉ IP (hay là địa chỉ máy chủ) và một dịch vụ được kiểm tra thêm, bổ sung thêm đến cùng một địa chỉ máy chủ. Ví dụ, một đối tượng như máy chủ có thể chỉ ra một địa chỉ IP 127.0.0.1 và một dịch vụ gọi là SSH. Trong cấu hình cài đặt Nagios này sẽ thực hiện một kiểm tra máy chủ trên một địa chỉ cục bộ (địa chỉ: 127.0.0.1) và khai báo thêm việc kiểm tra kết nối TCP tại cổng 22 sẽ thành công và một phiên kết nối SSH được thiết lập.

Cơ chế kiểm tra có thể chia thành hai loại chính: kiểm tra chủ động và kiểm tra bị động. Kiểm tra chủ động có nghĩa là Nagios phải kiểm tra theo những khoảng thời gian đã quy định để xem kết quả trả về là gì. Kiểm tra bị động nghĩa là lần lượt Nagios không tự bắt đầu những kiểm tra, mà chờ đợi một kết quả được kiểm tra trả về từ một ứng dụng hay một quá trình xử lý bên ngoài.

3.5.4 Quan hệ cha con

Quan hệ cha con trong Nagios là rất quan trọng. Một máy chủ con phụ thuộc vào một máy khác được xem như máy chủ cha, nghĩa là nếu máy chủ cha không hoạt động thì máy chủ con cũng không hoạt động được. Trong Nagios chỉ có định nghĩa máy chủ cha. Sau đó, Nagios mô tả những mối quan hệ này và phát họa thành bản đồ quan hệ từ chúng. Hơn nữa trong mối quan hệ giữa những máy chủ, Nagios

cũng mô tả và diễn giải những mối quan hệ giữa những dịch vụ trên máy chủ. Một máy chủ có thể tồn tại mà không có dịch vụ, nhưng một dịch vụ thì luôn luôn phải gắn kèm với một máy chủ. Mối quan hệ cha con đã cho thấy điều tốt nhất nếu một máy chủ cha tạo ra một thông báo cảnh báo, thì Nagios sẽ xem những dịch vụ và những máy chủ đằng sau nó và sẽ không tạo một cảnh báo cho chúng. Điều đó quan trọng nếu một thiết bị mạng switch không hoạt động, thì trong trường hợp này Nagios chỉ tạo một cảnh báo cho thiết bị mạng switch, và sẽ không gửi số lượng lớn cảnh báo về kết quả kiểm tra của tất cả các máy chủ không hoạt động đến người quản trị viên.

3.5.5 Các trạng thái của Nagios

Nagios có 4 trạng thái về kết quả kiểm tra dịch vụ: OK, Warning, Critical, và Unknown (theo thứ tự tăng dần). Những trạng thái này lần lượt có một loại trạng thái, Soft (mềm) hoặc Hard (cứng). Trạng thái mềm nghĩa là một kiểm tra máy chủ hoặc dịch vụ được trả về giá trị khác giá trị OK, nhưng một thông báo không được gửi. Tham số cấu hình max_check_attempts điều khiển việc kiểm tra có thể trả về bao nhiêu lần cùng một giá trị không OK trước một thông báo được gửi. Ví dụ những kết quả kiểm tra máy chủ là: UP, DOWN và Unreachable. Giá trị UP và DOWN cho biết kết quả của một máy chủ trực tiếp, trong khi Unreachable là kết quả được kiểm tra máy chủ từ máy chủ cha. Nếu máy chủ cha không hoạt động, Nagios biết được kết quả các máy chủ con cũng không hoạt động, vì vậy khai báo là chúng Unreachable.

Bảng 3.1 Bảng các mức độ cảnh báo trong Nagios

OK	WARNING	CRITICAL	UNKNOW

3.5.6 Những kiểu khai báo Macro

Kiểu Marco mang thông tin có thể được sử dụng trong những phần khác của cấu hình. Ví dụ, khi định nghĩa một lệnh kiểm tra cho lệnh ICMP ping, và có thể định nghĩa một địa chỉ máy chủ như một macro đến cấu hình của lệnh.

```
define host {
     host_name           localhost
     use                 linux-server
     alias               localhost
     address             127.0.0.1
     register            1
     }

define command {
       command_name      check_ping
       command_line      $USER1$/check_ping -H HOSTADDRESS$
                         -w $ARG1$ -c $ARG2$ -p 5
     }

define service {
     host_name           localhost
     service_description     PING
     use                 local-service
     check_command       check_ping!100.0,20%!500.0,60%
     register            1
     }
```

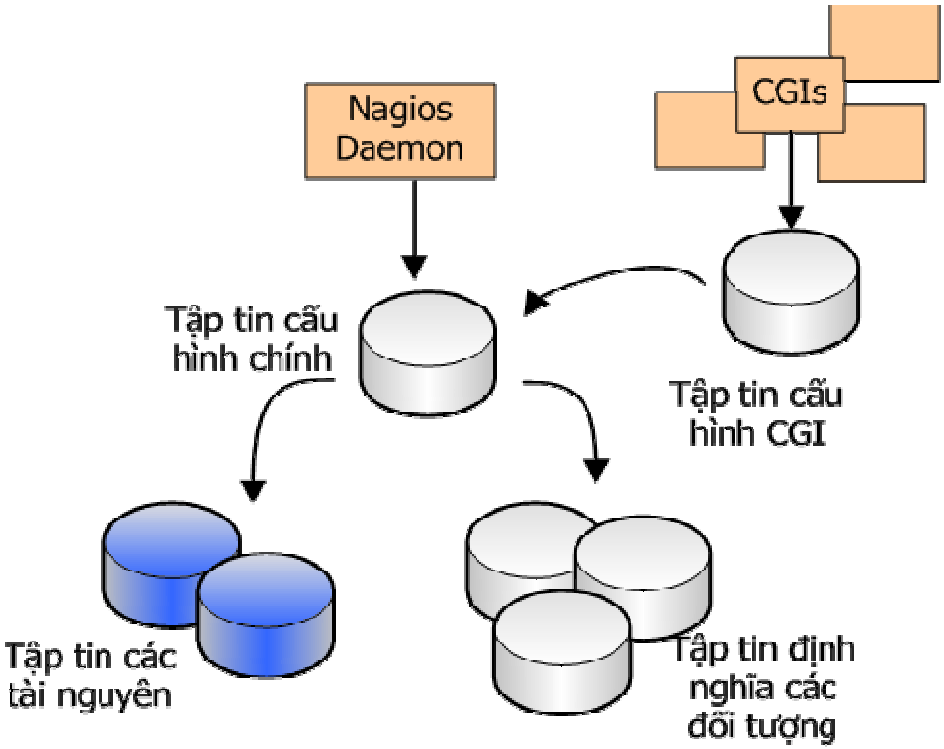
Hình 3.1 Ví dụ kiểu khai báo Macro

Trong hình bên trên, các macro được sử dụng trong định nghĩa lệnh để gọi hệ thống tập tin dẫn đến nơi thực thi có cài sẵn trong Nagios ($USER1$) và cung cấp một đối số đích đến lệnh ($HOSTADDRESS$). Trong trường hợp này, macro $HOSTADDRESS$ có địa chỉ tương ứng là 127.0.0.1 đã được định nghĩa trong định nghĩa máy chủ với tham số là address (địa chỉ).

3.5.7 Kiến trúc Nagios

Nagios có thể chia làm 4 loại chính: cấu hình chính (main configu-ration), các tài nguyên (resources), những định nghĩa đối tượng và cấu hình CGI (Common Gateway Interface – giao diện cổng ra vào chính). Cấu hình chính định nghĩa dịch

vụ Nagios hoạt động như thế nào. Các tài nguyên bao gồm những macro, hoạt động như các biến giúp đỡ trong cấu hình. Những định nghĩa đối tượng bao gồm các máy chủ, nhóm máy chủ, các dịch vụ, các nhóm dịch vụ, những đầu mối liên lạc, các nhóm liên lạc và các lệnh kiểm tra. Cấu hình CGI định nghĩa mặt trước của Nagios hoạt động như thế nào. Tổng quan cấu hình Nagios được hiển thị ở hình sau

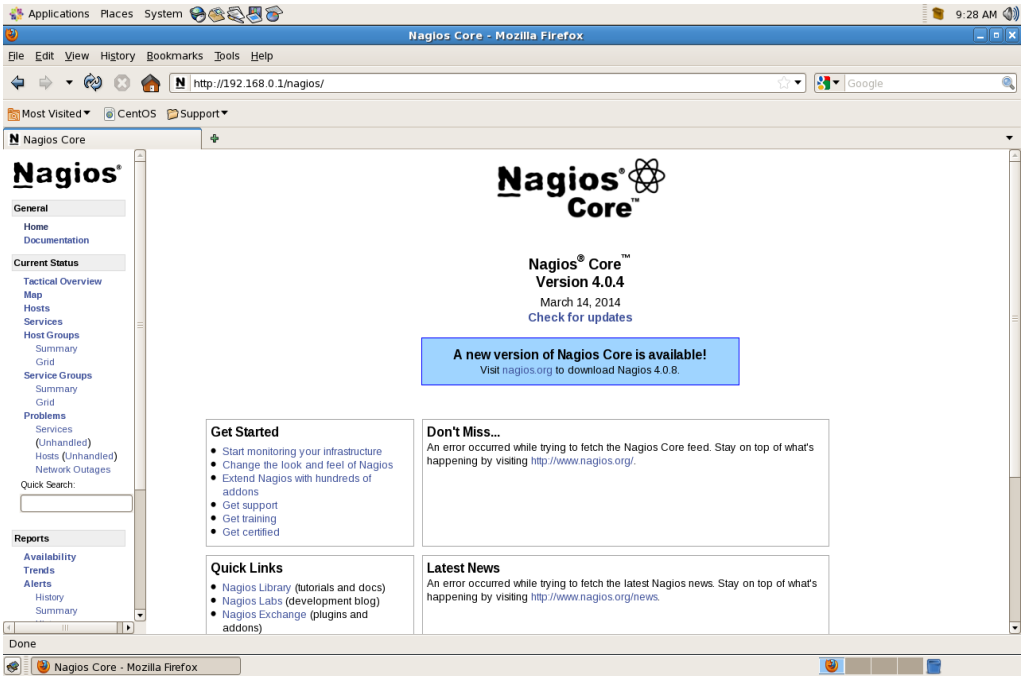


Hình 3.2 Mô tả kiến trúc của Nagios

Gói mã nguồn Nagios được kèm với những tập tin cấu hình ví dụ, các phần khác của cấu hình cũng được chia thành nhiều tập tin khác nhau. Những ví dụ này rất có lợi khi tạo một cấu hình đầu tiên thực sự, bởi vì chúng được định nghĩa nhiều dịch vụ khác nhau dựa trên những gói đã cài sẵn rồi. Như vậy, đó là cách tốt nhất để tạo ra một loại cấu hình tốt nhất cho Nagios, và không chỉ thay thế những giá trị chính trong những tập tin này.

3.5.8 Giao diện Nagios

Giao diện web Nagios được quản trị viên dùng để xem các trạng thái hiện tại của các máy chủ và các dịch vụ. Nó cung cấp một màn hình thống kê tổng quan để hiển thị một tổng hợp những vấn đề hiện tại, một bản đồ mà hiển thị các mối quan hệ của các máy chủ, các danh sách dịch vụ và máy chủ, các danh sách nhóm dịch vụ và nhóm máy chủ, và các danh sách các sự cố. Hơn nữa, cũng có thể chạy các lệnh từ giao diện web. Ví dụ, người quản trị có thể lập lịch thời gian chết cho một máy chủ hoặc một dịch vụ nếu biết sẽ có những thông báo bị ngắt, vô hiệu hóa đối với các máy chủ hoặc các dịch vụ đang tiếp tục không hoạt động với các lý do đã biết và nhận ra vấn đề đã xảy ra. Những báo cáo trạng thái các máy chủ hay các dịch vụ có thể được tạo ra và lịch sử các sự kiện có thể liệt kê ra để xem những cảnh báo mới nhất.



Hình 3.3 Giao diện chính của Nagios

Nagios không có sẵn dịch vụ máy chủ HTTP, mà nó sử dụng phần mềm dịch máy chủ Apache HTTP. Giao diện web Nagios được xây dựng trên các tập tin thực thi CGI và tập tin HTML tĩnh. Những tập tin CGI cần một bộ phận đặc biệt trong

phần mềm Apache hoạt động. Những tập tin CGI là những chương trình cơ bản nhỏ sinh ra mã code HTML. Những tập tin thực thi CGI đọc và diễn giải tập tin trạng thái Nagios và hiển thị thông tin hiện tại của Nagios.

3.6 Công cụ hỗ trợ tích hợp của Nagios

3.6.1 Công cụ Nagios

Nagios được gọi là một chương trình quan sát mạng, dịch vụ, và máy chủ mã nguồn mở. Thực sự, công cụ này là một bộ khung để quan sát các thiết bị, cho phép người quản trị viên nhanh chóng tập hợp nhiều dòng lệnh vào cấu hình để thu thập các thông tin. Bổ sung nhiều công cụ hỗ trợ Nagios ở ngoài, và dễ dàng tích hợp Nagios với các công cụ quan sát có thể sử dụng như công cụ NRPE, và MRTG.

Đầu tiên, điều cần thiết là lấy thông tin chủ yếu xoay quanh cấu hình chung của Nagios, nên cần bắt đầu với các tập tin cấu hình đơn giản liên quan đến bốn tập tin cấu hình như tập tin hosts, host groups, contacts, và services. Những tập tin cài đặt có sẵn mô tả ý nghĩa cụ thể các chức năng hoạt trong từng tập tin. Những tập tin được chứa trong thư mục cài đặt mặc định của Nagios /usr/local/nagios/etc.

Cấu hình của Nagios rất đơn giản, những máy chủ chạy cùng một dịch vụ có thể nhóm với nhau để quản trị viên dễ thống kê trong giao diện web Nagios. Tương tự, nhiều quản trị viên quản lý những dịch vụ khác nhau, thì thể nhóm các quản trị viên vào contact groups. Nếu một máy chủ chạy chương trình Nagios bị tắt hoặc mất kết nối một dịch vụ đang chạy thì Nagios thông báo quản trị viên hay nhóm quản trị viên quản lý máy chủ hoặc dịch vụ biết.

3.6.2 Nagios plugin

Các plugin của Nagios được xây dựng, đóng góp từ cộng động sử dụng Nagios. Đây là các module có tính năng nhất định, hầu hết được cung cấp bởi cộng đồng người sử dụng nagios, các chuyên gia, nhà quản trị mạng… thông qua trang web chính http://www.nagios.org/download/plugins, phiên bản mới nhất là “nagios-plugins-2.0.3.tar”. Trong phiên bản này chứa hầu hết đầy đủ các module

tính năng dùng giám sát hệ thống máy chủ để đánh giá hiệu suất sử dụng hiện tại. Tuy nhiên, vẫn còn một số tính năng cần thiết chưa được xây dựng hoặc còn một số hạn chế, ví dú như: tính năng phát hiện tấn công…Do đặc điểm mã nguồn mở nên người dùng có thể xây dựng lại các tính năng đã có cho phù hợp với thực trạng, yêu cầu riêng hay phát triển các tính năng mới cho hệ thống mà mình quản lý. Đây là điểm mạnh nổi trội của công cụ này.

3.6.3 Yêu cầu hệ thống

3.6.3.1 Phần cứng

Yêu cầu chạy Nagios chỉ là máy chủ chạy hệ điều hành Linux hoặc Unix và ngôn ngữ C. Những máy chủ cũng được cấu hình chạy giao thức TCP/IP khi kiểm tra các dịch vụ đạng hoạt động trên mạng.

3.6.3.2 Phần mềm

a. Nagios Core

b. Nagios Plugin

c. Dịch vụ web trên máy chủ (Apache)

d. Thư viện Zlib (libzlib, libzlib-devel)

e. Thư viện PNP (libpnp, libpnp-devel)

f. Thư viện Jpeg (libjpeg, libjpeg-devel)

g. Biểu tượng của các thiết bị

h. Công cụ NPRE

3.6.4 Đặc tính

Nagios chạy như một dịch vụ quan sát, kiểm tra những máy chủ và những dịch vụ, những công cụ hỗ trợ bên ngoài chỉ định để thu thập những thông tin chuyển về máy chủ chạy Nagios theo thời gian định kỳ được thiết lập sẵn. Khi phát hiện dấu hiệu các vấn đề xảy ra thì Nagios cảnh báo cho người quản lý hệ thống

thông qua e-mail hay một tin nhắn. Tất cả thông tin trạng thái về thời gian, những ghi nhận lịch sử, và các bảng báo cáo đều được gửi lên giao web để xem chi tiết.

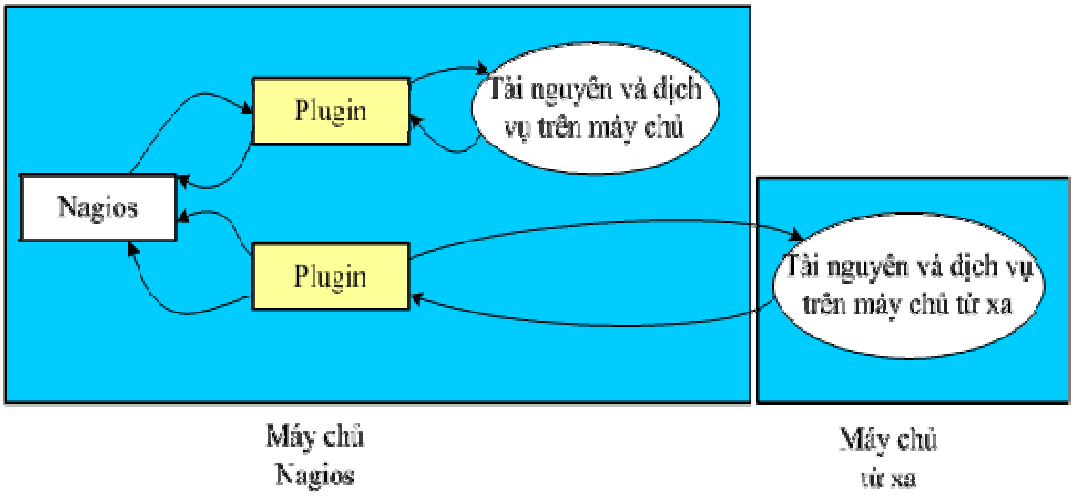
Một số đặc tính Nagios bao gồm

a. Quan sát các dịch vụ mạng (SSH, HTTP, PING, SMTP, POP3…)
b. Quan sát các tài nguyên của các máy chủ (tải sử dụng CPU, RAM, dung lượng sử dụng đĩa cứng…)
c. Những công cụ hỗ trợ Nagios đơn giản cho phép người quản trị dễ dàng phát triển những kiểm tra các dịch vụ chạy trên máy chủ từ xa cần quan sát (những kiểm tra dịch vụ song song).
d. Khả năng định nghĩa phân cấp máy chủ trong mạng bằng cách sử dụng những máy chủ "cha mẹ", điều đó phép phát hiện và phân biệt giữa những máy chủ không hoạt động và những máy chủ không thể kết nối được.
e. Những thông báo đến người quản trị khi một dịch vụ hay một máy chủ xảy ra vấn đề liên quan và gửi thông báo qua email, giao diện web, hay là những phương thức mà người quản trị có thể cài đặt.
f. Khả năng định nghĩa những phương thức đối xử các sự kiện chạy trong suốt quá trình các dịch vụ và máy chủ gặp sự cố liên quan.
g. Tự động xoay vòng sao lưu các tập tin ghi nhận thông ở nơi lưu trữ.
h. Hỗ trợ các máy chủ quan sát thực hiện liên tục khi có một máy chủ không hoạt động.
i. Lựa chọn sử dụng giao diện web để xem tổng quan trạng thái hiện giờ của mạng, lịch sử vấn đề và thông báo đã xảy ra, và tập tin ghi nhận thông tin đã yêu cầu, v.v…

3.6.5 Cơ chế hoạt động của Nagios

Ứng dụng Nagios chạy trên một máy chủ tập trung, như Linux hay Unix. Mỗi máy chủ quan sát phải chạy dịch vụ Nagios để giao tiếp với những máy chủ tập trung. Các tập tin cấu hình trên máy chủ tập trung được thực thi, sẽ tiến hành những kiểm tra cần thiết trên máy chủ từ xa và gửi thông tin lấy được về máy chủ tập trung. Trong khi ứng dụng phải chạy trên máy chủ Linux hay Unix, thì các máy chủ từ xa có thể là bất cứ phần cứng, hệ điều hành nào với điều kiện có thể giao tiếp được máy chủ chạy ứng dụng Nagios.

Tùy thuộc vào việc trả lời từ các máy chủ từ xa, Nagios sẽ đáp ứng với một hành vi thích hợp, và thêm lần nữa theo cấu hình cài đặt của nó. Tùy thuộc vào kiểm tra từ xa sẽ cần thực hiện cái gì, Nagios sẽ thực hiện kiểm tra thông qua khả năng của một máy chủ đó (như kiểm tra xem tập tin đó có tồn tại hay không), hoặc sẽ chạy một chương trình tinh chỉnh kiểm tra (gọi là công cụ hỗ trợ Nagios) để kiểm tra điều gì khó khăn hơn (như kiểm tra xem giá trị của phiên bản phần mềm nào đó). Nếu giá trị trả về không đúng thì Nagios sẽ tăng mức cảnh báo thông qua một vài phương thức đã định nghĩa và được cấu hình.



Hình 3.4 Hoạt động của Nagios

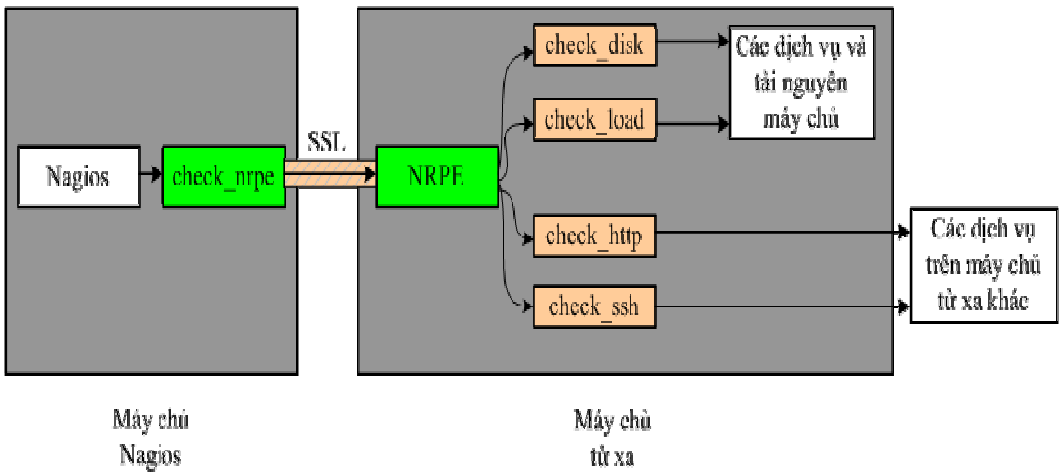
3.6.6 Công cụ hỗ trợ NRPE

3.6.6.1 Mục đích

Công cụ NRPE được thiết kế để cho phép người dùng thực thi những công cụ hỗ trợ Nagios trên các máy chủ Linux/Unix từ xa. Lý do chính cho phép Nagios quan sát những tài nguyên tại máy chủ này (như CPU, dung lượng bộ nhớ sử dụng, v.v.) trên những máy chủ từ xa. Bởi vì những tài nguyên này không thường xuyên được tiếp xúc ra bên ngoài, nên một chương trình chạy ngầm (gọi là agent) như NRPE phải được cài đặt trên những máy chủ chạy Linux hay Unix từ xa.

Ngoài ra, Nagios có thể thực thi các công cụ hỗ trợ Nagios trên các máy chủ Linux hay Unix từ xa bằng SSH, có một công cụ hỗ trợ *check_by_ssh* cho phép chúng ta làm điều này. Việc sử dụng SSH thì bảo mật hơn công cụ NRPE, nhưng nó sẽ tiêu hao tài nguyên CPU lớn hơn trên cả hai máy chủ quan sát và máy chủ từ xa. Đó là vấn đề khi sử dụng hàng trăm hay hàng ngàn máy chủ quan sát. Vì vậy, sử dụng công cụ NRPE là tốt hơn bởi vì nó sử dụng tải CPU ít hơn.

3.6.6.2 Mô hình hoạt động của Plugin



Hình 3.5 Mô hình hoạt động của plugin

Công cụ NRPE bao gồm hai phần:

- Công cụ hỗ trợ *check_nrpe* nằm trên máy chủ quan sát

- Dịch vụ NRPE sẽ chạy trên máy chủ Linux/Unix từ xa.

Khi Nagios cần quan sát tài nguyên một dịch vụ của một máy chủ Linux/Unix từ xa:

- Nagios sẽ thực thi công cụ hỗ trợ *check_nrpe* và cài đặt cho nó biết cần kiểm tra dịch vụ nào ở máy chủ từ xa.

- Công cụ hỗ trợ check_nrpe liên lạc với dịch vụ NRPE trên máy chủ từ xa thông qua một kênh kết nối, kênh đó được bảo vệ bởi giao thức bảo mật SSL.

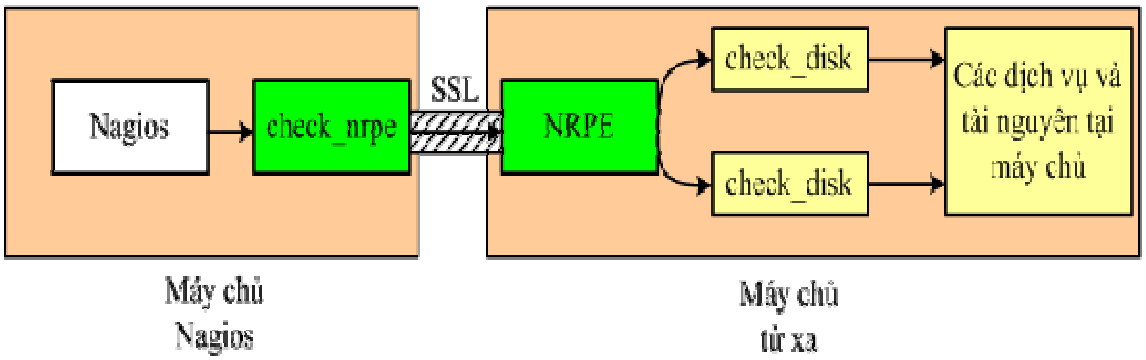
- Dịch vụ NRPE chạy công cụ hỗ trợ Nagios thích hợp để kiểm tra dịch vụ hay là những tài nguyên đã được cài đặt trước. Công cụ hỗ trợ Nagios này phải được cài đặt sẵn trên các máy chủ từ xa. Nếu không có công cụ này thì dịch vụ NRPE không thể quan sát bất cứ thứ gì trên máy chủ.

- Kết quả kiểm tra dịch vụ được dịch vụ NRPE trả về công cụ hỗ trợ check_nrpe, và công cụ này tiếp tục trả về cho phần mềm Nagios xử lý.

Hoạt động Nagios có thể tạo ra hai cách kiểm tra:

a. Sử dụng kiểm tra trực tiếp

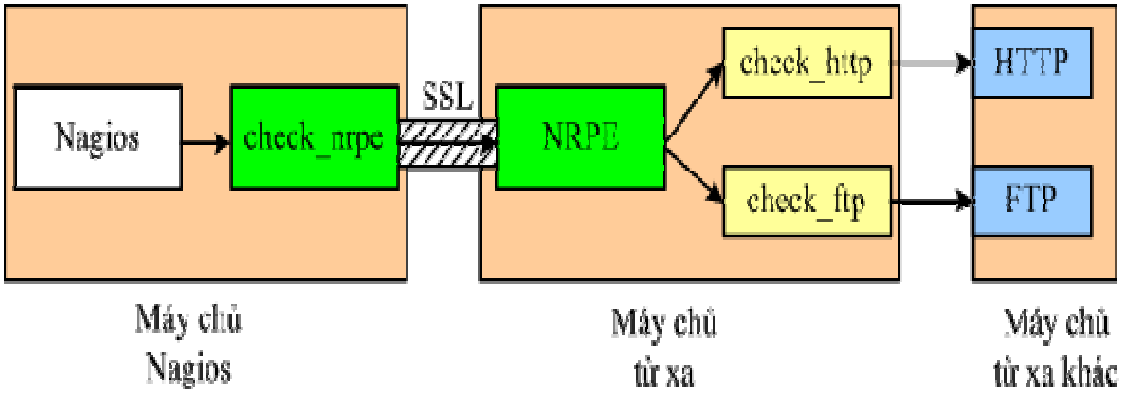
Đơn giản nhất sử dụng công cụ NRPE để quan sát những tài nguyên riêng trên tại máy chủ từ xa. Ví dụ như: tải CPU, RAM sử dụng, dụng lượng lưu trữ,…



Hình 3.6 Phương thức kiểm tra trực tiếp của Nagios

b. Sử dụng kiểm tra gián tiếp

Nagios có thể sử dụng công cụ NRPE để kiểm tra gián tiếp những dịch vụ và những tài nguyên công cộng của những máy chủ từ xa mà máy chủ Nagios không thể kết nối trực tiếp. Ví dụ, nếu máy chủ từ xa đã được cài đặt dịch vụ NRPE và công cụ hỗ trợ Nagios thì có thể giao tiếp với máy chủ từ xa khác (ngược lại máy chủ Nagios thì không thể), thì quản trị viên có thể cấu hình dịch vụ NRPE cho phép máy chủ Nagios quan sát máy chủ từ xa khác một cách gián tiếp. Dịch vụ NRPE quan trong hoạt động như một dịch vụ trung gian.



Hình 3.7 Phương thức kiểm tra gián tiếp của Nagios

3.7 Xây dựng plugin cảnh báo tấn công cho Nagios

Tính năng này được xây dựng nhằm phát hiện ra các dấu hiệu ban đầu khi tin tặc sử dụng các phương pháp tấn công riêng lẻ hay phối hợp chúng lại với nhau nhằm tránh phát hiện. Việc nghiên cứu xây dựng tính năng này nhằm tích hợp vào Nagios Core để phát hiện máy chủ bị tấn công từ chối dịch vụ kịp thời. Với tính năng này, người giám sát hệ thống có thể thay đổi, tùy chỉnh theo từng thời điểm cho phù hợp với tình trạng hệ thống mạng hiện tại. Đồng thời, có thể linh hoạt thay đổi, cập nhật các dấu hiệu tấn công tương ứng với từng phương pháp tấn công mà tin tặc sử dụng.

Để có thể phát hiện kịp thời các cuộc tấn công bất ngờ với tần suất lớn ngay tại thời điểm đầu tiên, cần phải quan sát thu thập các dấu hiệu bất thường trong quá trình thiết lập kết nối (đây là quá trình đầu tiên trong quá trình giao tiếp của máy tính bằng giao thức hướng kết nối TCP). Trong giai đoạn thiết lập kết nối, máy khách gửi các thông điệp TCP_SYN để yêu cầu máy chủ chấp nhận kết nối. Sau khi nhận được thông điệp này, máy chủ sẽ hồi đáp bằng thông điệp TCP_SYN/ACK và dành tài nguyên để dùy trì bán kết nối này trong khoảng thời gian 75 giây để chờ phản hồi TCP_ACK từ máy khách. Việc máy khách không gửi lại thông điệp TCP_ACK sẽ khiến cho máy chủ lãng phí tài nguyên để duy trì bán kết nối này. Ngoài ra, số lượng TCP_SYN được gia tăng một cách đột biến bởi số lượng lớn các máy khách tham gia vào quá trình này sẽ gây cạn kiệt tài nguyên máy chủ một cách nhanh chóng. Nguyên lý này được các tin tặc khai thác triệt để bằng nhiều kỹ thuật tấn công khác nhau, phối hợp nhiều kỹ thuật lại với nhau nhằm tránh phát hiện và gây khó khăn cho quá trình đối phó, khắc phục.

3.7.1 Phát hiện dấu hiệu tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ DoS là phương thức gia tăng đột biến lưu lượng trên đường truyền (băng thông) bằng cách cách gửi số lượng lớn yêu cầu kết nối dịch vụ đến máy chủ, làm cho máy chủ không đủ khả năng đáp ứng, dẫn đến dịch vụ của hệ thống bị đình trệ hay mất kiểm soát. Cuộc tấn công DoS là mối đe dọa

hiện nay, mặc dù đã có một số phương thức chống lại loại tấn công này nhưng vẫn chưa hiệu quả hay hiệu quả không cao.

Phương thức tấn công này được xây dựng trên nguyên lý thiết lập kết nối (ba bước bắt tay) từ máy khách đến máy chủ. Dựa vào nguyên lý này, một kiểu tấn công phổ biến được hình thành, đó chính là kiểu tấn công SYN. Hệ thống tấn công sẽ gửi yêu cầu SYN với địa chỉ IP nguồn giả (địa chỉ không tồn tại) , các yêu cầu SYN này là hợp lệ. Do đó, thong điệp ACK sẽ không bao giờ được gửi trả lại đến các máy nạn nhân, do đó số lượng bán kết nối mà máy nạn nhân phải duy trì là rất lớn [7]. Việc phòng chống phương pháp tấn công yêu cầu hệ thống phải nhận diện ra được dấu hiệu cơ bản ngay tại thời điểm đầu của cuộc tấn công. Phương thức phát hiện dựa trên các thuật toán phát hiện bất thường.

Các phương pháp phát hiện các dấu hiệu bất thường được xem xét bởi nhiều thông số đi kèm, ví dụ như CUSUM đi kèm thông số tổng tích lũy trung bình, và các cặp thông điệp xuất hiện tại giai đoạn truyền dữ liệu (cặp thông điệp SYN và FIN), hay các cặp thông điệp SYN và ACK…Tuy nhiên, các phương pháp này được áp dụng trên môi trường là các bộ định tuyến biên. Ngoài ra để có thể xây dựng được tính năng phát hiện tấn công từ chối dịch vụ tốt, cần phải xây dựng được bộ lọc gói tin. Để đánh giá được tính năng có phát hiện sớm dấu hiệu tấn công, và độ chính xác cao hay không phụ thuộc rất lớn vào bộ lọc gói tin này

Một trong các thuật toán được xây dựng để dò tìm sự bất thường là Adaptive Threshold Algorithm. Đây là một thuật toán đơn giản, dễ dàng triển khai và cài đặt, thích hợp trong môi trường Linux. Thuật toán này sẽ đo lưu lương gói TCP-SYN tại thời điểm đầu tiên của quá trình giao tiếp (quá trình thiết lập kết nối) và so sánh với giá trị ngưỡng được thiết lập trước. Đây chính là điểm khác biệt của thuật toán này so với các phướng pháp phát hiện dấu hiệu bất thường khác. Ngưỡng này được thiết lập trong khoảng thời gian nhất định dựa trên số lượng trung bình ước tính của gói TCP-SYN. Nếu lưu lượng đo vượt qua giá trị ngưỡng này thì đây chính là dấu hiệu bất thường và cảnh báo sẽ được kích hoạt.

Giả sử, xét tại thời điểm *t:*

x_t *: số lượng gói SYN nhận được trong khoảng thời gian thứ t*

μ_{t-1} *: tốc độ đo trung bình trước thời điểm t*

Điều kiện cảnh báo sẽ được thiết lập như sau:

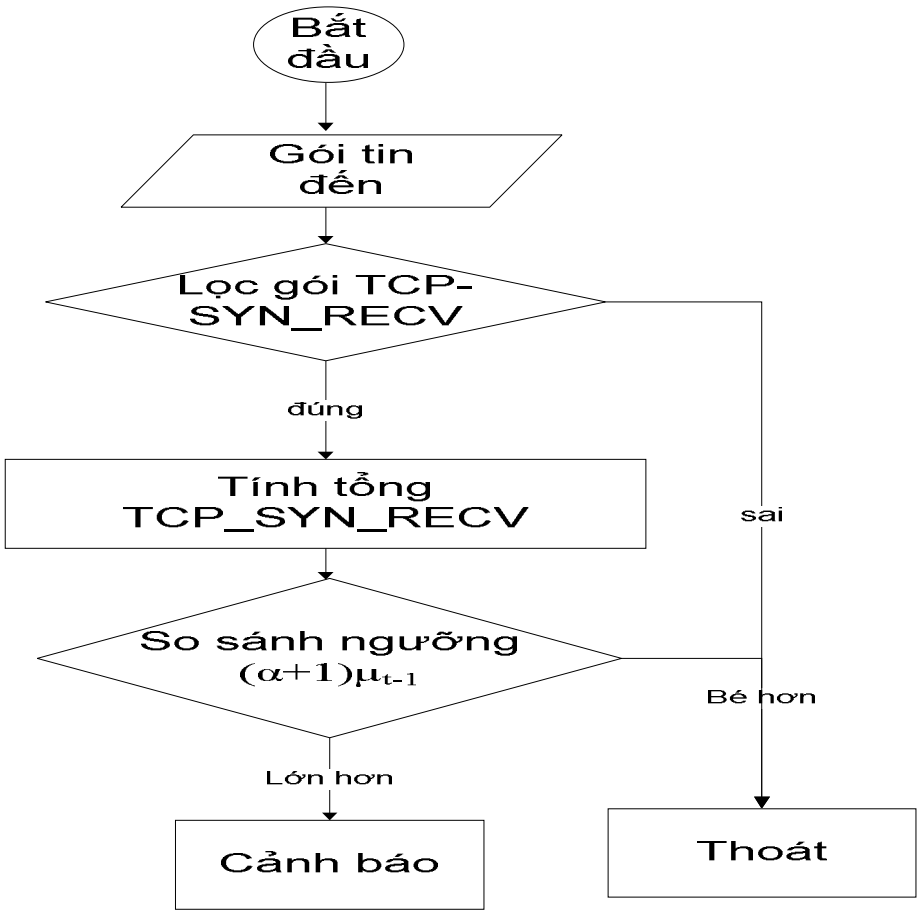
Nếu $x_t \geq (\alpha + 1)\, \mu_{t-1}$, *thì cảnh báo tại thời điểm t.*

Với :

μ_t *: giá trị ngưỡng trung bình được tính thông qua một số các mẫu thử sau một số khung thời gian.*

$\alpha > 0$ *: tỉ lệ phần trăm vượt ngưỡng trung bình của các mẫu thử vượt ngưỡng sau một số khung thời gian.*

Sơ đồ mô tả thuật toán Adaptive Threshold Algorithm dung để phát hiện dấu hiệu tấn công SYN được miêu tả như sau:



Hình 3.8 Sơ đồ thuật toán thiết lập ngưỡng thích nghi

Dựa vào sơ đồ này, đối với mỗi gói tin đến, đều được kiểm tra để xác định là gói TCP-SYN hay không. Nếu đúng, số lương gói TCP-SYN sẽ được cập nhật, sau đó tính toán hai giá trị α và μ để tìm ra giá trị ngưỡng. So sánh số lượng gói TCP-SYN nhận được với ngưỡng này để xác định điều kiện cảnh báo.

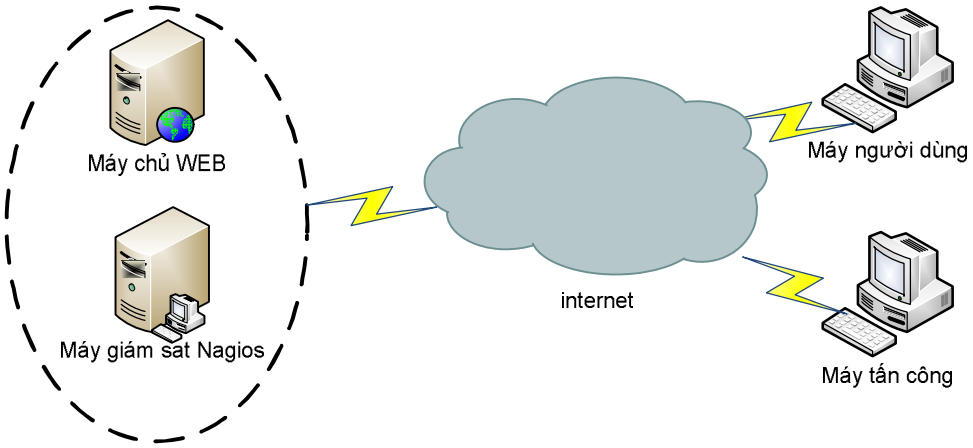
Đây là thuật toán khá đơn giản so với các thuật toán khác (ví dụ như CUSUM…) nhưng lại có hiệu quả cao trong việc dò tìm dấu hiệu của các cuộc tấn công từ chối dịch vụ lớn, với cường độ cao. Ưu điểm của phương pháp dò tìm này là thời gian phát hiện các dấu hiệu tấn công rất sớm, vì giám sát ngay quá trình đầu

tiên của quá trình giao tiếp. Bên cạnh đó, thuật toán rất tương thích và dễ dàng cài đặt để tích hợp vào tính năng của công cụ mã nguồn mở Nagios.

CHƯƠNG 4: KẾT QUẢ THỰC NGHIỆM VÀ ĐÁNH GIÁ

4.1 Mô hình thực nghiệm

Kết quả thực nghiệm thu được dựa trên mô hình kết nối sau:



Hình 4.1 Sơ đồ thực nghiệm

- **Máy chủ WEB**
  - ✓ Hệ điều hành : CentOS
  - ✓ Vi xử lý: Core 2 Duo 2,1Ghz
  - ✓ Bộ nhớ: 1Gb
  - ✓ Dịch vụ: web
- **Máy giám sát Nagios**
  - ✓ Hệ điều hành : CentOS
  - ✓ Vi xử lý: Core 2 Duo 2,1Ghz
  - ✓ Bộ nhớ: 1Gb
  - ✓ Dịch vụ:dùng Nagios giám sát, phát hiện tấn công trên máy chủ web

Trong mô hình thực nghiệm này, các trường hợp truy cập bình thường vào máy chủ web và tấn công sẽ được thực hiện bởi các máy tính. Đối với truy cập bình thường của người dùng và tấn công sẽ có dấu hiệu khác biệt nhau, mục đích nhằm kiểm tra tính năng phát hiện tấn công được tích hợp vào công cụ Nagios. Nếu trường hợp có dấu hiệu tấn công xảy ra, tính hiệu cảnh báo sẽ được kích hoạt. Hai trường hợp kiểm nghiệm được thực hiện trong một khoảng thời gian nhất định kéo dài khoảng 2 phút. Và các giá trị trong trường hợp truy cập bình thường sẽ được sử dụng như là mẫu thử cho trường hợp còn lại.

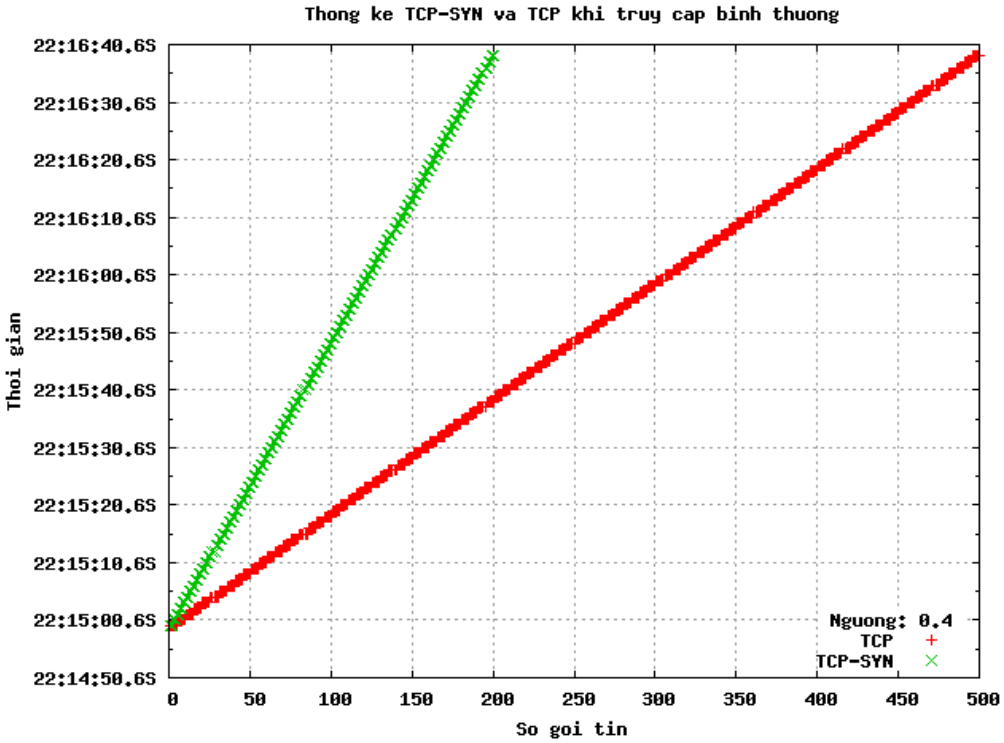
4.2 Phân tích, đánh giá kết quả thực nghiệm

4.2.1 Trường hợp truy cập bình thường

Khi người dùng truy cập dịch vụ bình thường, quá trình nối kết được thiết lập qua cơ chế bắt tay ba bước. Sau khi kết nối thành công và nhận được hồi đáp dịch vụ từ máy chủ, kết nối này vẫn được duy trì mở cho đến hết thời gian chờ (timeout) nên số lượng gói TCP-SYN để thiết lập kết nối lại là không cần thiết. Đặc điểm này được dựa tên tiêu chuẩn phiên bản HTTP 1.1 (persistent) mà máy chủ web đang hoạt động. Kết quả thu thập và rút trích từ công cụ TCPDUMP, số lượng gói tin TCP-SYN được gửi đến máy chủ nhằm thiết lập kết nối có tỉ lệ thấp hơn so với tỉ lệ tổng các gói TCP.

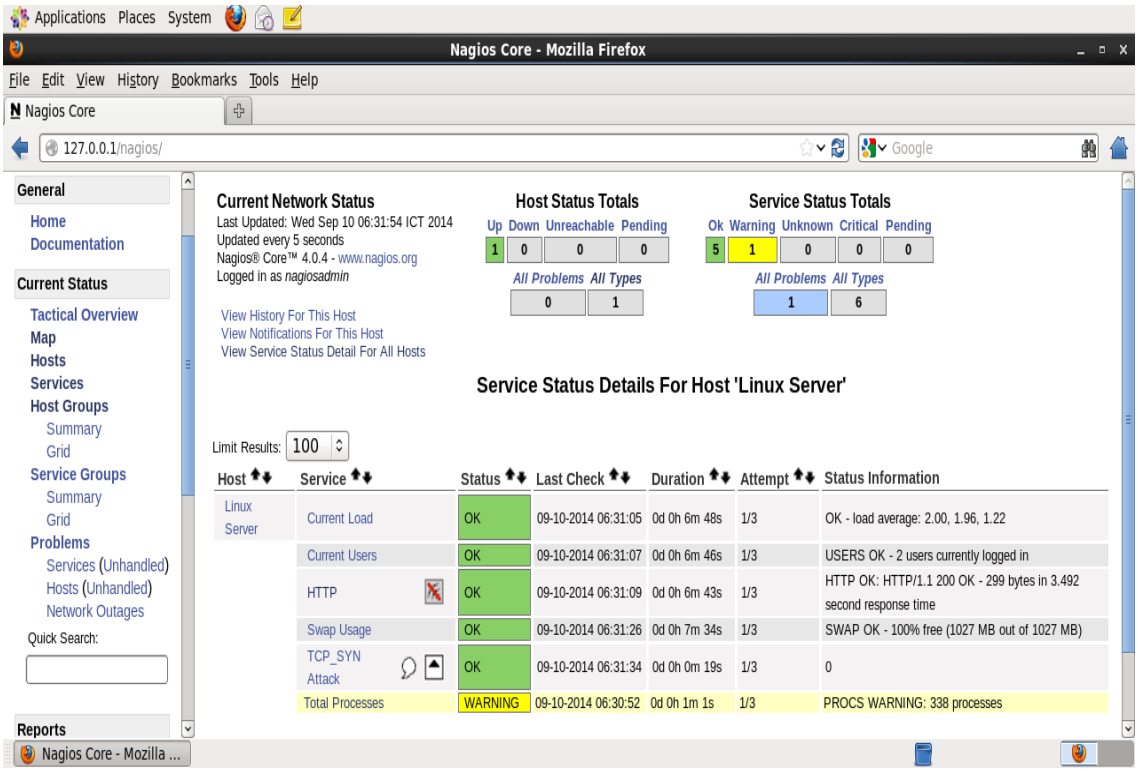
Bảng 4.1 Thống kê số lượng gói tin truy cập

Thời gian	Gói tin	
	TCP-SYN	TCP
~ 2 phút	200	500



Hình 4.2 Biểu đồ thống kê lưu lượng kết nối

Biểu đồ trên cho thấy kết quả thống kê tại thời điểm có kết nối bình thường. Kết quả thu thập được sau một khoảng khung thời gian (khoảng 2 phút), giá trị ngưỡng đạt được là $\alpha = 0.4$ (ngưỡng xác định tỉ lệ phần trăm trên tỉ lệ trung bình) và giá trị này sẽ được áp dụng như là ngưỡng an toàn để so sánh với các dấu hiệu tấn công sau này. Khi thực hiện giám sát trên công cụ Nagios theo thời gian thực, kết quả cho thấy đây là truy cập bình thường, không nguy hại và có cảnh báo an toàn (với mã là 0).



Hình 4.3 Kết quả cảnh báo trên Nagios khi kết nối bình thường

4.2.2 Trường hợp có tấn công xảy ra

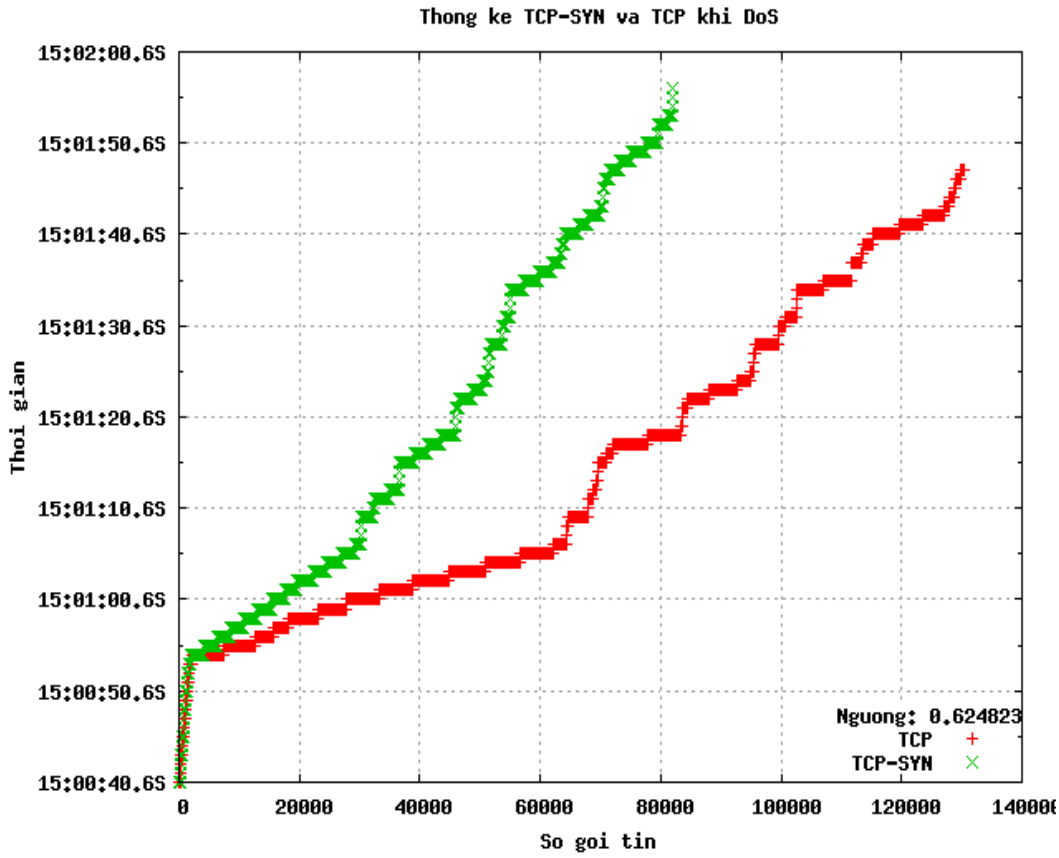
Trong trường hợp này, số lượng gói TCP-SYN được tạo ra với số lượng lớn hơn so với truy cập bình thường. Các lưu lượng có thể đến từ một nguồn hay nhiều nguồn khác nhau gây hại cho hệ thống. Trong trường hợp đến từ một nguồn thì đây là phương pháp tấn công từ chối dịch vụ SYN Flood. Trường hợp các gói TCP-SYN đến từ nhiều nguồn khác nhau thì đây là phương pháp tấn công loại DRDoS. Một trường hợp khác cũng gây ra tình trạng số lương gói TCP-SYN tăng đột biến và không kém phần nguy hiểm, đó chình là tấn công vào lớp ứng dụng, cụ thể là vào dịch vụ web của máy chủ và gây ra tình trạng giảm hiệu suất của máy chủ. Đó chính là phương thức tấn công HTTP-GET. Phương thức này tạo ra vô số kết nối thành công và liên tục gửi yêu cầu một trang trên máy chủ web, làm cho máy chủ phải luôn duy trì kết nối và đáp ứng trang được yêu cầu. Số lượng gói tin được thu thập và trích lọc từ công cụ TCPDUMP cho thấy tình trạng số lương gói TCP-SYN

gia tăng đáng kể. Đây là dấu hiệu bất thường cho thấy nguy cơ bị tấn công đang diễn ra. Trên thực tế, đối với hệ thống cỡ vừa, số lượng gói TCP-SYN đạt khoảng 500 gói tại một thời điểm cho thấy hệ thống đang bị tấn công.

Bảng 4.2 Thông kê số gói tin trong tình huống có tấn công

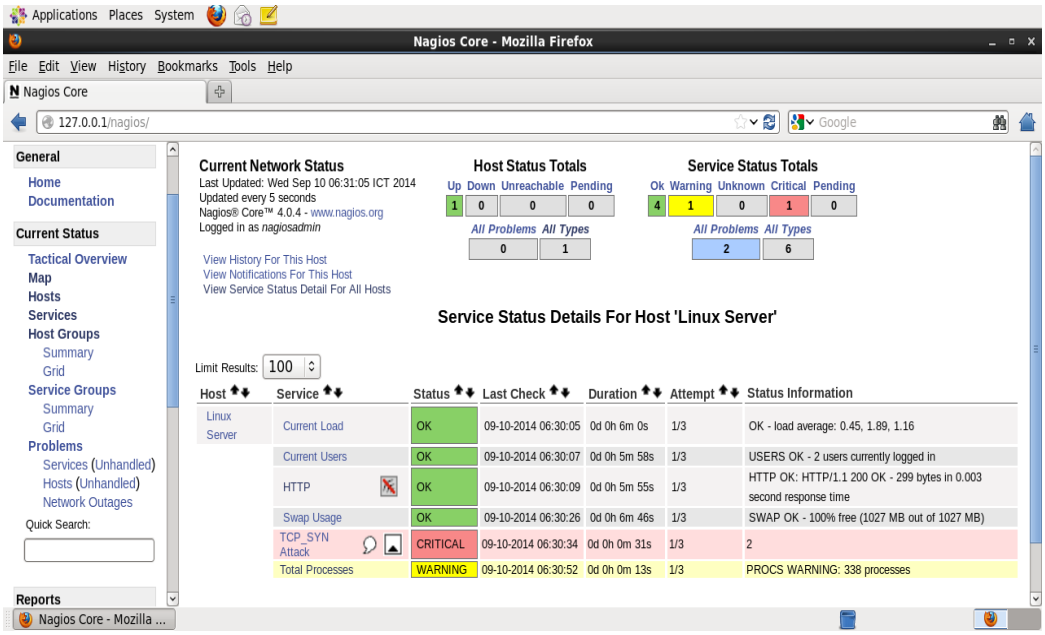
Thời gian	Gói tin	
	TCP-SYN	TCP
~ 2 phút	81904	130424

Trong tất cả các phương pháp trên và một số các phương pháp khác có cơ chế tương tự thì Nagios vẫn phát hiện ra được dấu hiệu tấn công. Kết quả thu thập trong khoảng thời gian khoảng 2 phút, giá trị ngưỡng đạt α = 0.624823, thời gian xác định tấn công ngay tại những thời điểm rất sớm đầu tiên. Ngưỡng này cao hơn so với trường hợp truy cập bình thường được sử dụng để làm mẫu, và đây chính là dấu hiệu chính để phát hiện ra tấn công.



Hình 4.4 Biểu đồ lưu lương khi tấn công

Biểu đồ trên cho thấy sự gia tăng đáng kể của lưu lương gói TCP-SYN trên kết nối theo thời gian. Đây là dấu hiệu bất thường vì theo nguyên tắc hoạt động của giao thức hướng kết nối, gói TCP-SYN được sử dụng trong giai đoạn đầu của bước thiết lập kết nối. Khi kết nối đã được thiết lập thì việc gửi thông điệp TCP-SYN là không cần thiết. Do có sự khác biệt bất thường về số lượng gói TCP_SYN xảy ra dựa vào giá trị ngưỡng, tính năng cảnh báo trên công cụ Nagios được thiết lập bằng mã 2 (Critical).



Hình 4.5 Kết quả cảnh báo có tấn công trên Nagios

Cảnh báo này được thiết lập theo thời gian thực nên đảm bảo được tính kịp thời, kèm theo các thông tin về hiệu suất có sẵn trong Nagios nên người quản trị mạng có được đầy đủ thông tin cần thiết để đánh giá và đưa ra biện pháp phòng chống, khắc phục kịp thời. Ngoài ra, khi các dấu hiệu tấn công thay đổi, người quản trị mạng cập nhật các dấu hiệu trong công cụ này.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Vấn đề an ninh mạng luôn là mối quan tâm hàng đầu hiện nay. Hệ thống mạng luôn đứng trước các nguy cơ tấn công không xác định trước từ tin tặc với nhiều phương pháp mới, kỹ thuật biến hóa, gây khó khăn trong việc đảm bảo hoạt động tốt của hệ thống mạng. Để có thể chủ động phòng ngừa hiệu quả và có các biện pháp khắc phục thích hợp khi có tấn công xảy ra, việc quan trọng cấp thiết nhất là phát hiện ra và cảnh báo kịp thời khi có dấu hiệu của các loại tấn công.

Với modelu tính năng phát hiện tấn công từ chối dịch vụ được xây dựng thành công trên môi trường mã nguồn mở, đã đóng góp một phần rất lớn trong lĩnh vực an ninh hệ thống. Giúp cho bộ công cụ Nagios trở nên mạnh mẽ hơn, hiệu quả khi được tích hợp tính năng phát hiện các dấu hiệu tấn công này vào, và cũng đã giải quyết được vấn đề một cách triệt để mà yêu cầu của luận văn đặt ra. Tính năng này hoạt động bằng phương pháp phát hiện ra các dấu hiệu bất thường trên số lượng lưu lượng truy cập phát sinh trong quá trình hoạt động của máy chủ. Một thuật toán đơn giản, dễ dàng cài đặt nhưng rất hiệu quả, cho kết quả ngay tại thời điểm đầu tiên của cuộc tấn công. Đây là một đóng góp lớn vào các phương pháp phát hiện tấn công, vì chỉ cần giám sát quá trình đầu tiên trong quá trình giao tiếp đã có thể phát hiện ra sự bất thường với độ chính xác cao. Bên cạnh đó, với các tính năng giám sát hiệu suất mạng sẵn có trong Nagios giúp cho người quản trị có được thông tin đầy đủ và chi tiết hơn để có thể phục vụ cho công việc quản trị hệ thống được tốt hơn.

Trong quá trình thực hiện luận văn, tôi đã tiến hành các tác vụ :

- Theo dõi và phân tích các dấu hiệu tấn công diễn ra trên hê thống mạng Trường Đại học Công Nghệ TPHCM.
- Nghiên cứu các phương pháp tấn công từ chối dịch vụ.

- Tìm hiểu các phương pháp phát hiện dấu hiệu tấn công.
- Cài đặt phần mềm Nagios Core
- Cài đặt, thiết lập các thông số phần mềm Nagios để giám sát máy chủ từ xa.
- Cài đặt và thiết lập thông số cho công cụ NRPE.
- Xây dựng plugin cảnh báo tấn công và tích hợp vào công cụ Nagios.
- Tiến hành triển khai thực nghiệm và phân tích, đánh giá kết quả đạt được.

Với những kiến thức mới tiếp thu được và kết quả đạt được của đề tài, tôi mong muốn một phần đóng góp vào việc giám sát và đảm bảo an ninh hệ thống mạng cho Trường Đại học Công Nghệ TPHCM. Hướng phát triển của đề tài trong tương lai sẽ tiếp tục phát triển những tính năng mới trên nền tảng mã nguồn mở trong lĩnh vực an ninh mạng, bảo mật hệ thống, nhằm phát hiện và cảnh báo kịp thời các dấu hiệu tấn công bằng các phương pháp mới, kỹ thuật tân tiến hơn.

TÀI LIỆU THAM KHẢO

[1] Muhammad Zakarya, (2013), "DDoS Verification and Attack Packet Dropping Algorithm in Cloud Computing", World Applied Sciences Journal 23 (11): 1418-1424, 2013

[2] G.S. Navale, Vivek kasbekar, Vijay ganjepatil, Shravanti bugade, (2014), "Detecting and analyzing ddos attack using map reduce in hadoop", International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982

[3] Tongguang Zhang, "Cumulative Sum Algorithm for Detecting SYN Flooding Attacks", Department of Computer and Information Engineering, Xinxiang College,Xinxiang, henan 453000, China.

[4] Haining Wang, Danlu Zhang, Kang G. Shin, Detecting SYN Flooding Attacks,EECS Department, The University of Michigan, Ann Arbor, MI 48109-2122

[5] Thwe thwe Oo, Thandar Phyu, "Classifying and identifying ddos attacks based on threshold verification technique", International Conference on Computer Networks and Information Technology.

[6] Paul J.Fortier, Howard E.Michel, (2003), " Computer System Performance Evaluation and Prediction", Digital Press, ISBN 1-55558-260-5.

[7] Mitko Bogdanoski, (2013), " Analysis of the SYN Flood DoS Attack", I. J. Computer Network and Information Securit, Published Online June 2013 in MECS (http://www.mecs-press.org/)

[8] S. Renuka Devi and P. Yogesh, "Detection of Application Layer DDoS Attacks Using Information Theory Based Metrics", department of information science and technology,college of engg. guindy, anna university, chennai. india.

[9] Xiao Zhenghong, Chen Zhigang, Deng Xiaoheng, (2010), "Anomaly Detection Based on a Multi-class CUSUM Algorithm for WSN", Journal of Computers, vol. 5, no. 2

[10] Junho Choi, Chang Choi, Byeongkyu Ko, Dongjin Choi, and Pankoo Kim, "Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment", Journal of Internet Services and Information Security (JISIS), volume: 3, number: 3/4, pp. 28-37.

[11] Anshul Kaushik, "Use of open source technologies for enterprise server monitoring using snmp", International Journal on Computer Science and Engineering, Vol. 02, No. 07, 2010, 2246-2252.

[12] Luis A. Trejo, Roberto Alonso, Adrián Ávila, Rául Monroy, Erika Sánchez, Jorge Vázquez, Mario Maqueo, "Using Cloud Computing MapReduce operations to Detect DdoS Attacks on DNS servers", http://homepage.cem.itesm.mx/raulm/netsec

[13] Mohamed Ibrahim AK and Lijo George, (2012), "Threshold Based Kernel Level HTTP Filter (TBHF) for DDoS Mitigation", I. J. Computer Network and Information Security, 2012, 12, 31-39

[14] Shweta Tripathi, Brij Gupta, Ammar Almomani, Anupama Mishra, Suresh Veluru, (2013), "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks", Journal of Information Security, 2013, 4, 150-164

PHỤ LỤC

TẬP TIN CẤU HÌNH DỊCH VỤ NAGIOS

```
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring the remote (Linux) host
        cfg_file=/usr/local/nagios/etc/objects/linuxserver.cfg
```

TẬP TIN CẤU HÌNH ĐỐI TƯỢNG, DỊCH VỤ GIÁM SÁT

```
# Define a host for the local machine

define host{
      use                linux-server          ; Name of host template to use
                                                 ; This host definition will inherit all
variables that are defined
                                                 ; in (or inherited by) the linux-server host
template definition.
      host_name            Linux Server
      alias              CentOS
      address              192.168.0.3
      }


# check syn attack
define service{
        use                              generic-service
```

```
        host_name               Linux Server
        service_description     TCP_SYN Attack
        check_command           check_nrpe!check_syn
        }
```

PLUGIN PHÁT HIỆN TẤN CÔNG

```
#!/usr/bin/perl -w

use Getopt::Std;



#################################



my %ERRORS = ('UNKNOWN' , '3',

            'OK' , '0',

            'WARNING', '1',

            'CRITICAL', '2' );

my $state = "UNKNOWN";

my $warning;

my $critical;


###################################

my %opts = ();

getopts("w:c:", \%opts);

if ((!$opts{w} || !$opts{c})) {

   print " -w <int>: Number of SYN_RECV warning.\n";

   print " -c <int>: Number of SYN_RECV critical.\n";
```

```
    exit (-1);
}
#####################################################
if ($opts{w}) {
    $warning = $opts{w};
}

if ($opts{c}) {
    $critical = $opts{c};
}
#####################################################
#program
#-------------
system("/bin/netstat -ant > /tmp/check_syn.txt");
my $syn = `grep SYN_RECV /tmp/check_syn.txt | wc -l`;
chomp $syn;
if ($syn >= $warning) {
        if ($syn >= $critical) {
                $state = "CRITICAL";
                print "2";
        } else {
                $state = "WARNING";
```

```
                print "1";

        }

} else {

        $state = "OK";

        print "0";

}

system("rm -f /tmp/check_syn.txt");

exit $ERRORS{$state};
```

CÔNG CỤ THỐNG KÊ THEO BIỂU ĐỒ GNUPLOT

```
set title "Thong ke TCP-SYN va TCP khi DoS"
set terminal png
set output 'kq-dos.png'
set grid
set autoscale
set key right bottom
set timefmt "%H:%M:%S"
set ydata time
set format y "%H:M:%S.%.6S"
set xlabel "So goi tin"
set ylabel "Thoi gian"
plot 'dos' using 1:2 title 'TCP', 'dos' using 1:3 title 'TCP-SYN'
```