BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

NGUYỄN THỊ THÙY TRANG

XÂY DỰNG HỆ THỐNG PHÁT HIỆN XÂM NHẬP MẠNG TRÊN NỀN ĐIỆN TOÁN ĐÁM MÂY

Chuyên ngành: Khoa học Máy tính
Mã số: 60.48.01.01

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

Đà Nẵng – Năm 2015

Công trình được hoàn thành tại

ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: TS. NGUYỄN TẤN KHÔI

Phản biện 1: PGS. TSKH. Trần Quốc Chiến

Phản biện 2: PGS. TS. Võ Thanh Tú

Luận văn đã được bảo vệ trước Hội đồng chấm Luận văn tốt nghiệp thạc sĩ kỹ thuật họp tại Đại học Đà Nẵng vào ngày 18 tháng 7 năm 2015

Có thể tìm hiểu luận văn tại:

- Trung tâm thông tin – Học liệu, Đại học Đà Nẵng
- Trung tâm Học liệu, Đại học Đà Nẵng

MỞ ĐẦU

1. Lý do chọn đề tài

Ngày nay với sự phát triển mạnh mẽ của công nghệ thông tin, mạng internet ra đời đã có những bước phát triển và ảnh hưởng lớn đến nhiều mặt của cuộc sống con người. Tuy nhiên những nguy cơ tiềm ẩn như thông tin cá nhân, thông tin doanh nghiệp được lưu trữ trên mạng internet ngày càng dễ bị xâm phạm, phá hủy nếu hệ thống mạng dùng để lưu trữ không được bảo vệ an toàn.Vì vậy cùng với sự phát triển các dịch vụ nền internet thì vấn đề an ninh, an toàn thông tin cũng là mối quan quan tâm hàng đầu của các công ty, các tổ chức và các nhà cung cấp dịch vụ [2], [15].

Trong vòng vài năm trở lại đây, điện toán đám mây – Cloud Computing đã và đang trở thành một trong những thuật ngữ được nhắc đến nhiều nhất trong ngành công nghệ thông tin. Điện toán đám mây được hứa hẹn là giải pháp giải quyết được nhiều vấn đề như độ sẵn sàng (availability), khả năng co giãn (scalability), chi phí (cost), điện năng tiêu thụ (power consumption). Điện toán đám mây phát triển mạnh và đã trở nên phổ biến với nhiều nhà cung cấp các tài nguyên tính toán dưới dạng dịch vụ như Microsoft, Amazon... khả năng quản lý tài nguyên tính toán tập trung, cấp phát và tính chi phí theo nhu cầu sử dụng đem lại sự tiện lợi, khả năng mở rộng dễ dàng cho người dùng [14].

Các kỹ thuật tấn công mạng hiện nay ngày càng tinh vi khiến các hệ thống an ninh truyền thống như tường lửa dần trở nên mất hiệu quả, các hệ thống này bảo vệ mạng theo cách cứng nhắc và không bảo vệ được hệ thống trước những tấn công mới. Một trong những giải phảp có thể đáp ứng hiệu quả cho vấn đề này là triển khai hệ thống dò tìm xâm nhập trái phép – Instruction Detect System

(IDS). Hệ thống có thể phát hiện các cuộc tấn công mạng từ cả bên ngoài lẫn bên trong. Hệ thống phát hiện xâm nhập IDS là một phương pháp bảo mật có khả năng chống lại các kiểu tấn công mới, các vụ lạm dụng xuất phát từ trong hệ thống và có thể hoạt động tốt với các phương pháp bảo mật truyền thống.Mặc dù được xem là một công cụ hiệu quả để bảo vệ mạng nhưng khi hoạt động các hệ thống IDS yêu cầu nhiều quá trình xử lý để phát hiện tấn công vì vậy có những giới hạn về khả năng xử lý lượng tin tại một thời điểm đối với một hệ thống mạng lớn [10].

Vì những lý do như trên, tôi chọn thực hiện đề tài *"Xây dựng hệ thống phát hiện xâm nhập mạng trên nền điện toán đám mây"* nhằm nghiên cứu đề xuất một giải pháp bảo vệ an toàn mạng dựa trên công nghệ điện toán đám mây và kỹ thuật IDS.

2. Mục tiêu và nhiệm vụ của đề tài

2.1. Mục tiêu

Mục tiêu chính của đề tài nhằm nghiên cứu xây dựng hệ thống phát hiện xâm nhập mạng trên nền tảng điện toán đám mây.

2.2. Nhiệm vụ

- Tìm hiểu về an toàn và bảo mật thông tin
- Tìm hiểu về điện toán đám mây
- Tìm hiểu cơ chế hoạt động của hệ thống phát hiện xâm nhập
- Triển khai đám mây sử dụng nền tảng OpenStack
- Xây dựng tập tin ảnh máy ảo cài sẵn phần mềm Snort
- Xây dựng mô hình cung cấp dịch vụ phát hiện xâm nhập
- Thử nghiệm và đánh giá mô hình triển khai

3. Đối tượng và phạm vi nghiên cứu

3.1. Đối tượng nghiên cứu

- Cơ sở lý thuyết về điện toán đám mây và hệ thống IDS.

- Cụ thể là hệ thống OpenStack và phần mềm IDS Snort.

3.2. Phạm vi nghiên cứu

- Các phương thức tấn công và cách phòng chống trên hệ thống phát hiện xâm nhập mạng.

- Công nghệ phát hiện xâm nhập mạng.

- Mô hình phát hiện xâm nhập trên nền điện toán đám mây.

4. Phương pháp nghiên cứu

Đề tài sử dụng các phương pháp nghiên cứu như sau:

4.1. Phương pháp lý thuyết

- Tổng hợp tài liệu về điện toán đám mây và hệ thống IDS

- Nghiên cứu các hệ thống điện toán đám mây tư nhân

- Nghiên cứu các kỹ thuật, phần mềm phát hiện xâm nhập mạng

- Đề xuất mô hình phát hiện xâm nhập trên điện toán đám mây

4.2. Phương pháp thực nghiệm

- Triển khai mô hình hệ thống

- Xây dựng hệ thống điện toán đám mây OpenStack

- Xây dựng các hệ thống máy ảo IDS Snort trên nền OpenStack

5. Ý nghĩa khoa học và thực tiễn

5.1. Ý nghĩa khoa học

- Phát triển hệ thống phát hiện xâm nhập mạng IDS trong an ninh mạng.

- Xây dựng hệ thống phát hiện xâm nhập mạng trên nền điện toán đám mây.

5.2. Ý nghĩa thực tiễn

Đề xuất giải pháp góp phần đảm bảo an toàn cho các dịch vụ trên nền điện toán đám mây.

6. Bố cục luận văn

Luận văn được trình bày bao gồm 3 chương như sau:

Chương 1: Tổng quan về đề tài, trình bày tổng quan về điện toán đám mây và nền tảng đám mây OpenStack. Giới thiệu về hệ thống phát hiện xâm nhập, phân loại nguyên lý hoạt động và phần mềm IDS mã nguồn mở Snort.

Chương 2: Hệ thống điện toán đám mây OpenStack, chương này trình bày về mô hình thiết kế và cài đặt triển khai một đám mây OpenStack và những vấn đề liên quan đến tạo mạng ảo trong OpenStack.

Chương 3: Xây dựng hệ thống IDSCloud, chương này bao gồm những vấn đề tồn tại hiện nay của các hệ thống IDS truyền thống, mô hình giải pháp đưa ra, đánh giá kết quả.

Kết luận và hướng phát triển đề tài: Đánh giá kết quả đạt được, xác định những ưu nhược điểm và hướng phát triển trong tương lai.

CHƯƠNG 1
TỔNG QUAN VỀ ĐỀ TÀI

1.1. ĐIỆN TOÁN ĐÁM MÂY

1.1.1. Giới thiệu

Hiện nay có nhiều cách định nghĩa về điện toán đám mây khác nhau, sau đây là một số định nghĩa về điện toán đám mây của những công ty, tổ chức uy tín:

Theo Wikipedia[20]: *"Điện toán đám mây là mô hình điện toán sử dụng các công nghệ máy tính và phát triển dựa vào mạng Internet. Mọi khả năng liên quan đến công nghệ thông tin đều được cung cấp dưới dạng các "dịch vụ", cho phép người sử dụng truy cập các dịch vụ công nghệ từ một nhà cung cấp nào đó "trong đám mây" mà không cần phải có các kiến thức, kinh nghiệm về công nghệ đó, cũng như không cần quan tâm đến các cơ sở hạ tầng phục vụ công nghệ đó."*

Theo Viện Tiêu chuẩn và Công nghệ (NIST) đã đưa ra nghĩa định nghĩa như sau [34]: *"Điện toán đám mây là một mô hình cho phép ở một vị trí thuận tiện, khách hàng có thể truy cập mạng theo yêu cầu và được chia sẻ tài nguyên máy tính (mạng, máy chủ, lưu trữ, ứng dụng và dịch vụ) được nhanh chóng từ nhà cung cấp. Trong trường hợp xấu nhất thì cũng phải cung cấp dịch vụ hoạt động ở mức tương tác".*

1.1.2. Mô hình tổng quan

Theo định nghĩa, các nguồn điện toán khổng lồ như phần mềm, dịch vụ ... sẽ nằm tại các máy chủ ảo (đám mây) trên Internet thay vì trong máy tính gia đình và văn phòng (trên mặt đất) để mọi người kết nối và sử dụng mỗi khi họ cần.

1.1.3. Đặc điểm của điện toán đám mây

Điện toán đám mây có 5 đặc điểm chính [6]:

- Dịch vụ tự đáp ứng theo yêu cầu (On-demand self-service)
- Khả năng truy cập diện rộng (Broad network access)
- Quản lý tài nguyên tập trung (Pooling resource management)
- Tính co dãn nhanh (Rapid Elasticity)
- Dịch vụ đo lường (Measured Service)

1.1.4. Các dịch vụ của điện toán đám mây

Điện toán đám mây hiện tại được chia ra làm ba dịch vụ cơ bản chính là: [5]

- Hạ tầng như một dịch vụ (IaaS)
- Nền tảng như một dịch vụ (PaaS)
- Phần mềm như là một dịch vụ (SaaS)

1.1.5. Các mô hình triển khai điện toán đám mây

- Mô hình đám mây công cộng (Public Cloud)
- Mô hình đám mây riêng (Private Cloud)
- Mô hình đám mây lai (Hybrid Cloud)
- Mô hình đám mây cộng đồng (Community cloud)

1.1.6. Những lợi ích của điện toán đám mây

- Tính linh động
- Giảm bớt phí
- Tạo nên sự độc lập
- Tăng cường độ tin cậy
- Bảo mật
- Bảo trì dễ dàng

1.1.7. Những hạn chế của điện toán đám mây

- Tính riêng tư
- Tính bảo mật

- Sự phụ thuộc
- Chất lượng dịch vụ (QoS)
- Tiết kiệm năng lượng
- Mất dữ liệu
- Sử dụng tài nguyên đám mây cho mục đích xấu
- Thiếu mô hình quản lý
- Hiệu năng thực tế

1.2. HỆ THỐNG PHÁT HIỆN XÂM NHẬP

1.2.1. Hệ thống phát hiện xâm nhập

Thuật ngữ *"xâm nhập"(Intrusion)* trong lĩnh vực bảo mật thông tin bao gồm cả các cuộc tấn công không thành công và các cuộc tấn công đã thành công tức là đã có ý niệm phân biệt giữa tấn công và xâm nhập [1].

Phát hiện xâm nhập"Intrusion Detection" là quá trình theo dõi các sự kiện xảy ra trong một hệ thống máy tính hoặc trong một hệ thống mạng. Sau đó phân tích các dấu hiệu của các sự cố có thể xảy ra để tìm ra dấu hiệu *xâm nhập*.

Hệ thống phát hiện xâm nhập "*Intrusion Detection Systems"* là một hệ thống giám sát lưu thông mạng và phòng chống, phát hiện các hành động tấn công vào một mạng.

1.2.2. Hệ thống IDS

IDS (Intrusion Detection System): Hệ thống phát hiện xâm nhập là một thiết bị phần cứng hoặc một phần mềm giúp giám sát các hoạt động trong mạng hoặc hệ thống để phát hiện các hoạt động gây hại hoặc vi phạm chính sách an ninh và gửi báo cáo về một trạm quản lý (Hình 1.6).

1.2.3. Các thành phần của một hệ thống IDS

IDS bao gồm các thành phần chính sau:

- Thành phần thu thập dữ liệu
- Thành phần tiền xử lý
- Thành phần phân tích
- Thành phần phản ứng

1.2.4. Nguyên lý hoạt động

Nguyên lý hoạt động của một hệ thống phòng chống xâm nhập được chia làm năm giai đoạn chính:

- Giám sát mạng (Monotoring)
- Phân tích lưu thông (Analyzing)
- Liên lạc
- Cảnh báo (Alert)
- Phản ứng (Response)

1.2.5. Chức năng chính của một hệ thống IDS

Hệ thống IDS có ba chức năng quan trọng nhất là: giám sát – cảnh báo – bảo vệ.

1.2.6. Phân loại các hệ thống IDS

- Host-based IDS (HIDS)
- Network-IDS (NIDS)
- Hệ thống phân tán IDS (DIDS)

1.2.7. Các phương pháp tấn công mạng

- Phương pháp tấn công từ chối dịch vụ DoS
- Vô hiệu hóa hệ thống
- Giả mạo địa chỉ
- Khai thác lỗi hệ thống
- Tấn công lỗ hổng bảo mật web

1.2.8. Các kỹ thuật phát hiện tấn công

- Phát hiện dựa trên sự lạm dụng/dấu hiệu
- Phát hiện dựa trên sự bất thường

1.2.9. Lợi ích của hệ thống IDS

- Hệ thống IDS có thể phát hiện tấn công từ trong cũng như bên ngoài mạng. IDS có thể giám sát, bảo vệ tất cả các cổng chạy các dịch vụ của hệ thống.

- IDS có khả năng quản lý tương quan các cuộc tấn công, cũng như khả năng phòng thủ theo chiều sâu. Ngoài ra còn giúp người quản trị có khả năng xác định số lượng tấn công và các thông tin về cuộc tấn công.

1.2.10. Hạn chế của hệ thống IDS

- Phải có sự nâng cấp, cập nhật cơ sở dữ liệu liên tục để hệ thống có thể làm việc hiệu quả.

- Có khả năng đưa ra các nhận định sai, đưa ra cảnh báo đối với hành vi bình thường và bỏ qua hành vi xâm nhập làm giảm hiệu năng hệ thống.

- Tốn chi phí lớn để triển khai đối với những khu vực mạng có lưu lượng dữ liệu cao.

1.3. PHẦN MỀM IDS NGUỒN MỞ SNORT

1.3.1. Giới thiệu

Snort là phần mềm IDS/IPS nguồn mở được phát triển bởi Sourcefire. Kết hợp việc kiểm tra dấu hiệu, giao thức và dấu hiệu bất thường, Snort đã được triển khai rộng khắp trên toàn thế giới.

Snort sử dụng các luật được lưu trữ trong các file text. Các luật được nhóm lại thành kiểu và lưu trữ dưới dạng các tập dữ liệu riêng. Người dùng có thể tự tạo các luật, sử dụng cơ sở dữ liệu luật thương mại hoặc sử dụng những bộ luật miễn phí do cộng đồng phát triển.

Snort hoạt động theo chế độ dòng lệnh có khả năng hoạt động phân tích dữ liệu trong mạng IP theo thời gian thực. Snort sẽ bắt và phân tích các gói tin, thu thập những thông tin cần thiết và so sánh

với cơ sở dữ liệu luật. Nếu phát hiện dấu hiệu xâm nhập trùng khớp với mẫu trong cơ sở dữ liệu, Snort sẽ tạo ra các cảnh báo.

1.3.2. Cơ chế hoạt động của Snort

Snort có 4 chế độ hoạt động:

- Chế độ Sniffer
- Chế độ Packet Logger
- Chế độ NIDS
- Chế độ Inline

1.3.3. Kiến trúc của Snort

Snort được chia thành nhiều thành phần. Một IDS dựa trên Snort bao gồm các thành phần chính sau đây:

- Bộ giải mã gói tin (Package Decoder)
- Bộ tiền xử lý (Preprocessor)
- Bộ phát hiện (Detection Engine)
- Bộ ghi nhật ký và cảnh báo
- Bộ kết xuất thông tin

1.3.4. Luật của Snort

a. Giới thiệu

Hầu hết các hành vi xâm nhập đều có những dấu hiệu nhận biết, những dấu hiệu này được sử dụng để định nghĩa tạo nên các luật cho Snort.

Một luật có thể được sử dụng để tạo nên một thông điệp cảnh báo, log một thông điệp hay có thể bỏ qua một gói tin.

b. Cấu trúc luật của Snort

Một luật Snort có dạng như sau:

alert ip any any -> any any (msg: IP Packet detected)

Một luật của Snort gồm có 2 phần chính đó là Rule Header và Rule Option.

Rule Header	Rule Option

- Header: là phần đầu của một luật trong Snort, chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin. Header cũng bao gồm hướng đi của gói tin đó.

- Phần Option: chứa thông điệp cảnh báo và các thông tin về các phần gói tin dùng để tạo cảnh báo. Các tiêu chuẩn phụ được khai báo trong phần tùy chọn sẽ giúp cho việc so sánh gói tin giúp cho một luật có khả năng phát hiện được nhiều khả năng tấn công khác nhau.

KẾT LUẬN CHƯƠNG 1

Trong chương này trình bày tổng quan về điện toán đám mây, hệ thống điện toán điện toán OpenStack, hệ thống IDS và phần mềm Snort.Từ đó đề xuất giải pháp xây dựng hệ thống phát hiện xâm nhập mạng trên nền tảng điện toán đám mây với mục tiêu tận dụng những thế mạnh của tài nguyên đám mây để tăng hiệu năng hoạt động của phần mềm Snort. Chương tiếp theo sẽ phân tích và xây dựng một hệ thống IDS trên nền tảng điện toán đám mây.

CHƯƠNG 2
HỆ THỐNG ĐIỆN TOÁN ĐÁM MÂY OPENSTACK

2.1. TỔNG QUAN VỀ OPENSTACK

2.1.1. Giới thiệu

OpenStack được NASA phối hợp cùng RackSpace phát triển từ năm 2010. Đây là một dự án điện toán đám mây nhắm đến việc cung cấp cơ sở hạ tầng như là một dịch vụ. OpenStack là mã nguồn mở được viết bằng ngôn ngữ Python và phát hành dưới giấy phép Apache.

Dự án OpenStack giúp các tổ chức cung cấp dịch vụ điện toán

đám mây chạy trên phần cứng tiêu chuẩn.

OpenStack bao gồm nhiều dự án liên quan đến nhau: bộ xử lý, lưu trữ, mạng trong một đám mây. Tất cả quyền quản lý có thể thực hiện qua cửa sổ dòng lệnh hoặc thông qua một giao diện bảng điều khiển web.

2.1.2. Các thành phần trong OpenStack

- Thành phần Compute (Nova)
- Thành phần lưu trữ đối tượng (Swift)
- Thành phần dịch vụ ảnh đĩa (Glance)
- Thành phần lưu trữ khối (Cinder)
- Thành phần quản lý mạng (Neutron)
- Thành phần Dashboard (Horizon)
- Thành phần chứng thực (Keystone)
- Thành phần Telemetry(Ceilometer)
- Thành phần Orchestration (Heat)

2.1.3. Ưu điểm của hệ thống OpenStack

- Hỗ trợ triển khai các mô hình đám mây tư nhân, công cộng, lai...
- OpenStack không phụ thuộc vào phần cứng độc quyền.
- Mô hình mạng linh hoạt có thể cấu hình phù hợp với yêu cầu người dùng.
- Có thể quản lý trực tiếp các máy ảo.
- Có thể gán hay thu hồi các địa chỉ IP đã cấp phát cho máy ảo.
- Linh hoạt trong việc kiểm soát truy cập các máy ảo.
- Có khả năng phân bổ, theo dõi và hạn chế việc sử dụng tài nguyên.
- Hỗ trợ truy cập VNC các máy ảo qua giao diện web Horizon.
- Cho phép tạo một ảnh máy ảo mới từ một máy ảo đang sử dụng.

2.1.4. Hạn chế của hệ thống OpenStack

- OpenStack hiện đang được phát triển vì vậy các phiên bản phát hành có sự thay đổi lớn khiến khách hàng liên tục phải cập nhật hệ thống.
- Hệ thống tài liệu OpenStack chưa được viết đầy đủ.
- Chỉ hỗ trợ kỹ thuật qua email và chat.
- Thiếu nhiều tính năng so với các hệ thống có bản quyền.

2.2. TRIỂN KHAI HỆ THỐNG OPENSTACK

2.2.1. Các thành phần cài đặt

Hệ thống đám mây được chọn triển khai trong luận văn là phiên bản OpenStack Folsom (2012) với bảy thành phần chính.

- Compute Nova
- Network Quantum
- Image Glance
- Dashboard Horizon
- Object Storage Swift
- Block Storage Cinder
- Identity Service Keystone

2.2.2. Cài đặt hệ thống OpenStack

Một hệ thống OpenStack thông dụng gồm có 3 thành phần Controller, Network và Compute sẽ được cài trên ba server chạy hệ điều hành Ubuntu Server 12.10 64 bit.

Các thành phần cài đặt cụ thể trên 3 server như sau:

- *Server Controller:* KeyStone, Glance, các dịch vụ của Nova, Horizon, Quantum Openvswitch Plugin, Quantum Server.
- *Server Network:* Quantum DHCP Agent, Quantum L3 Agent, Quantum Openvswitch Agent.
- *Server Compute:* Nova Compute, KVM, Quantum

Openvswitch Agent.

- Hệ thống có ba mạng riêng để các server gửi nhận dữ liệu:

- *Mạng Quản lý:* được sử dụng nội bộ trong hệ thống OpenStack dùng để quản lý các server có trong hệ thống. Những IP thuộc mạng này chỉ có thể truy cập từ trong trung tâm dữ liệu.

- *Mạng Dữ liệu:* là mạng kết nối giữa Compute và Network để truyền dữ liệu nội bộ bên trong kiến trúc đám mây. Đây là mạng để thành phần Nova làm việc với Quantum giúp các máy ảo bên trong server Compute có thể kết nối với mạng và trao đổi dữ liệu.

- *Mạng API:* là mạng có kết nối ra ngoài internet, cho phép người dùng truy cập các API của OpenStack qua mạng này từ bất kỳ đâu. Trong mô hình này mạng API cũng chính là mạng cho phép các máy ảo có thể truy cập ra mạng ngoài qua nó.

2.3. MẠNG RIÊNG TRONG OPENSTACK

2.3.1. Giới thiệu

Quantum là dịch vụ mạng ảo cung cấp API cho phép những thiết bị từ các dịch vụ khác như Compute có thể định nghĩa các kết nối.

Các thành phần của Quantum bao gồm: Quantum-server, quantum- agent, DHCP-agent, L3-agent, Queue.

2.3.2. Tạo một mạng riêng trong OpenStack

Để đảm bảo tính bảo mật nên triển khai một mô hình mạng riêng. Quantum hỗ trợ nhiều mô hình thiết kế mạng riêng khác nhau. Mạng riêng của tất cả người dùng được kết nối đến một router, router này được quản lý bởi nhà cung cấp và cho phép các mạng riêng kết nối ra mạng ngoài.

Trong mô hình này ta xây dựng hệ thống có 2 mạng trong đó mạng *ext* là mạng được dùng để kết nối ra ngoài internet và mạng *net_proj_one* là mạng được tạo ra cho người sử dụng *user_one* hình 2.5.

2.4. QUẢN LÝ MÁY ẢO

Horizon được phát triển với nhiệm vụ cung cấp cho người dùng giao diện sử dụng các dịch vụ khác của Openstack như nova, quantum...

Để tạo và quản lý các máy ảo ta có thể sử dụng giao diện đồ họa của Horizon bằng cách truy cập vào địa chỉ *192.168.100.51/horizon*.

Để khởi tạo các máy ảo vmsnort và vmgateway cần thực hiện:

- Tạo các khóa bảo mật
- Tạo các địa chỉ floating IP

Để khởi động các máy ảo ta cần thiết lập các thông số:

- Flavors
- Tập tin ảnh
- Mạng riêng
- Key security

KẾT LUẬN CHƯƠNG 2

Trong chương này trình bày việc triển khai một đám mây cung cấp tài nguyên dựa trên nền tảng OpenStack và nghiên cứu về hệ thống mạng trong OpenStack cũng như cách để khởi động một máy ảo từ giao diện quản lý web, đám mây này sẽ cung cấp tài nguyên là các máy tính ảo để phục vụ cho hệ thống phát hiện xâm nhập mạng.

CHƯƠNG 3
XÂY DỰNG HỆ THỐNG IDSCLOUD

3.1. MÔ TẢ BÀI TOÁN

Hệ thống IDSCloud được thiết kế và mô tả trong hình 3.1 bao gồm:

- Nền tảng đám mây OpenStack cung cấp tài nguyên là các máy tính ảo có khả năng phân tích dữ liệu mạng để phát hiện tấn công mạng. Các máy ảo này có thể được thuê với số lượng tùy ý, có

khả năng mở rộng cấu hình hoặc tùy chọn các cơ sở dữ liệu luật phù hợp với nhu cầu người dùng.

- Các máy server giám sát mạng cần bảo vệ có nhiệm vụ:

- Bắt và ghi dữ liệu của mạng cần bảo vệ.
- Vận chuyển dữ liệu mạng ghi được đến các máy ảo trên đám mây.
- Nhận kết quả phân tích từ đám mây và hỗ trợ giao diện đồ họa để người dùng có thể giám sát trực quan.

3.2. PHÂN TÍCH CHỨC NĂNG

Từ mô tả yêu cầu của mô hình đề xuất, hệ thống IDSCloud cần có những tính năng chính:

- Hệ thống IDSCloud
- Mở rộng theo yêu cầu
- Khả năng sử dụng linh hoạt
- Khả năng toàn quyền quản lý dữ liệu
- Khả năng tự quản lý CSDL luật
- Khả năng bảo mật

3.3. THIẾT KẾ HỆ THỐNG IDSCLOUD

3.3.1. Mô tả hệ thống

Hệ thống IDSCloud được đề xuất xây dựng hệ thống phát hiện xâm nhập mạng cung cấp đến người dùng như một dịch vụ từ đám mây.Trong mô hình đề xuất tài nguyên sử dụng phân tích phát hiện xâm nhập mạng được tách biệt khỏi hệ thống người dùng.

Hoạt động của hệ thống được mô tả như sau:

Bước 1: Dữ liệu mạng được thu thập từ máy người dùng.

Bước 2: Dữ liệu mạng thu thập được chuyển đến máy ảo cài đặt Snort trên hệ thống đám mây.

*Bước 3:*Máy ảo sẽ tiến hành phân tích, phát hiện dấu hiệu xâm

nhập và gửi trả kết quả phân tích về máy người dùng.

3.3.2. Các thành phần chính của hệ thống

Hệ thống IDSCloud được thiết kế như hình trên với 5 thành phần chính hình 3.3:

- Thành phần bắt gói tin
- Thành phần vận chuyển gói tin
- Thành phần phân tích gói tin
- Thành phần lưu trữ kết quả
- Thành phần giám sát, thống kê

3.3.3. Các yêu cầu của hệ thống

- Xây dựng đám mây cung cấp tài nguyên
- Tích hợp phần mềm IDS vào máy ảo
- Xây dựng đường truyền dữ liệu an toàn
- Giám sát dữ liệu tập trung

3.3.4. Các công cụ triển khai trên hệ thống

- Cơ sở hạ tầng điện toán đám mây OpenStack
- Hệ thống phát hiện xâm nhập Snort
- Công cụ StrongSwan

3.3.5. Hoạt động của hệ thống IDSCloud

Cơ chế hoạt động chính của hệ thống:

- Toàn bộ thông tin ra vào trên hệ thống mạng 192.168.119.0/24 của người sử dụng sẽ được giám sát bởi máy Monitor.

- Thông tin bắt từ mạng được lưu ghi vào một tập tin và sau một khoảng thời gian được tự động chuyển đến máy ảo vmSnort trên nền đám mây để thực hiện phân tích tìm dấu hiệu xâm nhập.

- Kết quả phân tích sẽ được máy vmSnort trả về về cơ sở dữ liệu trung tâm đặt tại máy Monitor.

- Người quản trị mạng/giám sát tại máy Monitor có thể theo dõi kết quả phát hiện xâm nhập qua giao diện Web.

- Khi có phát hiện xâm nhập hoặc tấn công, hệ thống sẽ cảnh báo thông qua giao diện, hoặc gửi thông tin hoặc kích hoạt chế độ bảo vệ tự động sử dụng tường lửa IPTable.

3.4. KẾT QUẢ TRIỂN KHAI THỰC NGHIỆM

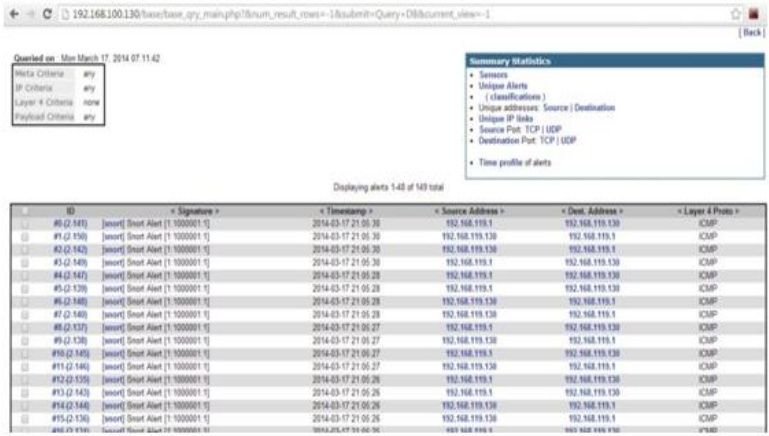
3.4.1. Kịch bản 1 – Phát hiện và cảnh báo

Sau khi triển khai hệ thống như hình 3.5 và truy cập vào giao diện quản lý của BASE qua địa chỉ máy Monitorhttp: //192.168.100.130/base ta có thể theo dõi kết quả giám sát hoạt động trong mạng 192.168.119.0/24 do máy vmSnort đưa về.

Thử nghiệm với một luật tạo cảnh báo khi ping đến một máy thuộc lớp mạng bảo vệ như sau:

alert icmp any any ->any any (msg: "ICMP"; sid:1000001; rev:1;)

Khi tiến hành ping máy 192.168.119.130 tại giao diện BASE ta có thể thấy kết quả như hình 3.7



Hình 3.7. Giao diện trang web giám sát BASE

Tại máy vmSnort ta có thể thấy cảnh báo được tạo ra như hình 3.8

Hình 3.8. Màn hình tại máy ảo vmSnort

Tại máy Monitor ta có thể thấy được Deamonlogger tạo các tập tin pcap và SnortManager chuyển tập tin đến máy vmSnort

Hình 3.9. Màn hình Daemonlogger tại máy Monitor

```
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470616
File transfered
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470695
ket noi den client
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470664
File transfered
3879
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470731
ket noi den client
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470695
File transfered
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470766
ket noi den client
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470731
File transfered
3879
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470821
ket noi den client
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470766
File transfered
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470856
ket noi den client
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470821
File transfered
3879
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470911
ket noi den client
chuyen file/home/lhnam/logdir/daemonlogger.pcap.1397470856
File transfered
3879
ENTRY_CREATE: /home/lhnam/logdir/daemonlogger.pcap.1397470946
ket noi den client
```

Hình 3.10. Màn hình SnortManager tại máy Monitor

3.4.2. Kịch bản 2–Đánh giá hiệu năng của hệ thống IDS Cloud

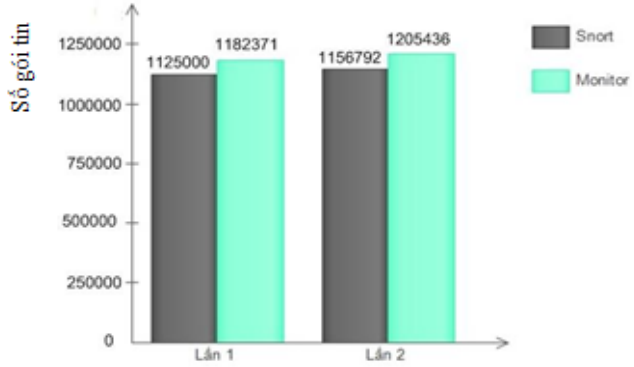
Để đánh giá hiệu năng của hệ thống, ta tiến hành so sánh kết quả phát hiện xâm nhập trên IDSCloud với kết quả phát hiện trên một máy IDS Snort đơn (địa chỉ 192.168.119.113) không sử dụng hạ tầng đám mây Hình 3.11.

Ta cài đặt máy Monitor sử dụng IDSCLoud và máy IDS Snort đơn. Cả hai máy này sẽ cùng giám sát mạng 192.168.119.0/24 để phát hiện xâm nhập mạng. Máy Client (192.168.119.100) sẽ thực hiện việc gửi dữ liệu để 2 máy giám sát cùng phân tích. Tất cả 3 máy Client, Snort, Monitor đều có cấu hình giống. Khả năng phân tích gói tin dựa trên cùng 1 phiên bản Snort và cơ sở dữ liệu luật.

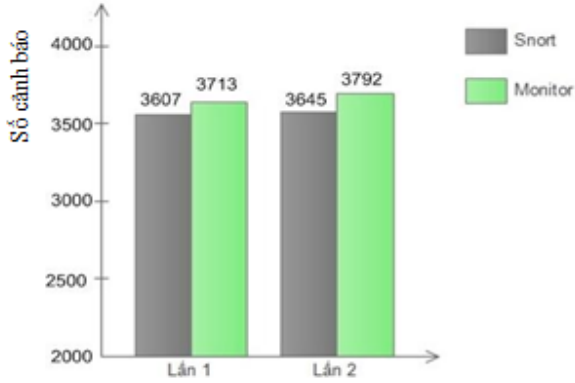
Máy Monitor sẽ liên lạc với máy vmSnort qua địa chỉ floating IP 192.168.100.103 được gắn vào máy vmSnort.

Sử dụng tập tin pcap chứa dữ liệu để phân tích chứa 1.220.246 gói tin mạng, tạo ra 3823 cảnh báo khi sử dụng với CSDL luật Snort được cài. Máy Client sẽ thực hiện gửi các gói tin vào mạng từ tập tin pcap nhờ vào công cụ Bittwist.

Thực hiện kịch bản thử nghiệm hai lần và đánh giá trên số lượng gói tin bắt được và số cảnh báo phát hiện ta được kết quả thống kê thể hiện như trong hình 3.12 và hình 3.13.



Hình 3.12. Kết quả số lượng gói tin bắt được trong mạng



Hình 3.13 Kết quả số lượng cảnh báo tạo ra

Số lượng gói tin thực trong mạng có thể lớn hơn số gói tin

trong tập tin pcap tuy nhiên những gói tin này không ảnh hưởng đến số cảnh báo được tạo ra vì vậy trong kịch bản thử nghiệm này không đánh giá số gói tin rớt mà chỉ đánh giá số gói tin đã nhận và số cảnh báo phát hiện được.

Qua kết quả ta có thể thấy được máy Monitor sử dụng IDSCloud có khả năng bắt được nhiều gói tin hơn và phát hiện được nhiều mối nguy hiểm hơn so với máy Snort sử dụng mô hình Snort truyền thống.

3.4.3. Ưu điểm của mô hình

- Đáp ứng được với mạng tốc độ cao
- Khả năng mở rộng:

3.4.4. Nhược điểm của mô hình

- Sự phụ thuộc tốc độ kết nối:
- Tốc độ phản hồi chậm:

KẾT LUẬN CHƯƠNG 3

Trong chương này trình bày về giải pháp sử dụng tài nguyên máy ảo do đám mây cung cấp để phục vụ phân tích dữ liệu mạng nhằm phát hiện các mối nguy hiểm tấn công mạng và đánh giá mô hình thử nghiệm. Kết quả cho thấy mô hình đã giải quyết được những yêu cầu đề ra tuy nhiên vẫn còn những hạn chế cần được nghiên cứu phát triển hoàn thiện thêm.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. KẾT QUẢ ĐẠT ĐƯỢC

Sau thời gian tìm hiểu và nghiên cứu để tìm ra giải pháp triển khai hệ thống phát hiện xâm nhập mạng trên nền điện toán đám mây hoạt động hiệu quả hơn hệ thống truyền thống, luận văn đã đạt được những kết quả sau:

Về mặt lý thuyết

– Tìm hiểu và nghiên cứu về điện toán đám mây, những ưu nhược điểm của các dịch vụ đám mây, xu hướng phát triển của điện toán đám mây trên thế giới vànền tảng đám mây nguồn mở OpenStack.

– Tìm hiểu về các hệ thống phát hiện xâm nhập mạng.

– Nghiên cứu về những vấn đề bất cập trong những hệ thống phát hiện xâm nhập hiện tại và những đề xuất một giải pháp IDS Cloud mới.

– Nghiên cứu đề xuất giải pháp sử dụng nguồn tài nguyên tính toán cung cấp từ đám mây để xây dựng hệ thống phát hiện xâm nhập.

Về mặt thực tiễn

Luận văn đã xây dựng mô hình hệ thống phát hiện xâm nhập trên nền tảng điện toán đám mây với những kết quả sau:

– Triển khai đám mây sử dụng nền tảng OpenStack cung cấp các máy tính ảo được tích hợp sẵn phần mềm IDS Snort.

– Xây dựng mô hình thử nghiệm và đánh giá việc dùng máy ảo trên đám mây để phục vụ phân tích dữ liệu mạng nhằm phát hiện sớm các cuộc tấn công.

2. KIẾN NGHỊ VÀ HƯỚNG PHÁT TRIỂN

Tiếp tục phát triển hệ thống theo hướng tìm cách đơn giản hóa việc triển khai để người dùng có thể cài đặt triển khai một cách dễ dàng, nghiên cứu tích hợp phần gửi nhận dữ liệu mạng vào module DAQ của Snort. Nghiên cứu triển khai những mô hình Snort phân tán sử dụng nhiều máy ảo để tăng tốc độ của hệ thống IDSvà đáp ứng được mạng tốc độ cao.

Cải thiện các luật trong hệ thống Snort và trong chương trình, xây dựng hệ thống cảnh báo đa dạng, để nâng cao độ chính xác phát hiện xâm nhập. Cần triển khai thử nghiệm trên mạng wireless. Bên cạnh đó cũng cần thiết xây dựng các luật Snort đủ mạnh có khả năng nhận diện và phát hiện chính xác được những hình thức tấn công mới.