HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

LÊ MẠNH CƯỜNG

NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN XÂM NHẬP TÍCH HỢP CHO MẠNG LAN

CHUYÊN NGÀNH : **HỆ THỐNG THÔNG TIN**

MÃ SỐ: **8.48.01.04**

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. HOÀNG XUÂN DẬU

HÀ NỘI - 2021

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. Hoàng Xuân Dậu

Phản biện 1: PGS.TS. Trần Đình Quế

Phản biện 2: TS. Tạ Quang Hùng

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

Vào lúc: 15 giờ ngày 28 tháng 08 năm 2021

Có thể tìm hiểu luận văn tại:

Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Hiện nay các cuộc tấn công xâm nhập ngày càng tận dụng các lỗ hổng, điểm yếu của hệ thống một cách tinh vi, gây ra mối đe dọa tới sự an toàn thông tin. Các cuộc tấn công có thể đến từ nhiều hướng theo các cách khác nhau, do đó cần phải đưa ra các chính sách và biện pháp đề phòng cần thiết. Mục đích cuối cùng của an toàn bảo mật hệ thống thông tin và tài nguyên theo các yêu cầu sau:[1]

- Đảm bảo tính bí mật (*Confidentiality*): Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền.
- Đảm bảo tính nguyên vẹn (*Intergrity*): Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.
- Đảm bảo tính sẵn dùng (*Availability*): Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền.
- Đảm bảo tính không thể từ chối (*Non-repudiation*): Thông tin được cam kết về mặt pháp luật của người cung cấp.

Luận văn này nghiên cứu các về xâm nhập hệ thống thông tin và các giải pháp phát hiện xâm nhập hệ thống, phân tích đặc tính, phương thức hoạt động, đánh giá ưu nhược điểm và tính ứng dụng trong thực tế. Luận văn bao gồm 3 chương với nội dung sau:

Chương I: Tổng quan về xâm nhập và phát hiệm xâm nhập. Trình bày tổng quan xâm nhập, các dạng tấn công xâm nhập và hệ thống phát hiện xâm nhập.

Chương II: Các hệ thống phát hiện xâm nhập. Trình bày các hệ thống phát hiện xâm nhập mạng, xâm nhập host và xâm nhập tích hợp. Giới thiệu một số hệ thống tiêu biểu, thành phần, chức năng và so sánh các hệ thống này.

Chương III: Thử nghiệm triển khai giải pháp phát hiện xâm nhập tích hợp Security Onion cho mạng LAN. Trình bày về các bước triển khai, cài đặt thành phần phát hiện xâm nhập của hệ thống Security Onion. Thử nghiệm chạy thử với một số kịch bản tấn công xâm nhập phổ biến.

CHƯƠNG I. TỔNG QUAN VỀ XÂM NHẬP VÀ PHÁT HIỆN XÂM NHẬP

Chương I trình bày về định nghĩa tấn công, xâm nhập hệ thống, khái quát các phương thức sử dụng, mục tiêu và tác hại của nó. Tiếp đó sẽ phân loại các dạng tấn công, xâm nhập và giới thiệu các phương thức tiêu biểu.

1.1. Tổng quan về xâm nhập

Trong suốt những năm qua, chúng ta đã chứng kiến sự bùng nổ của mạng Internet thương mại, gieo mầm cho mạng kỹ thuật số toàn cầu có tính tương tác, đã tạo ra những thứ từ email đến việc chữa bệnh từ xa, từ trình duyệt đến các mạng xã hội, từ ngân hàng trực tuyến cho đến thương mại điện tử rất phổ biến và tiện dụng.

Với những bước đổi mới đáng kể của công nghệ mạng đã giúp chúng ta dễ dàng thu thập và chia sẻ thông tin hơn và mang lại rất nhiều giá trị cho con người. Khi những công nghệ này ngày càng phổ biến rộng rãi, chi phí đổi mới giảm xuống, đồng nghĩa với việc người tiêu dùng, các doanh nghiệp vừa và nhỏ, thậm chí rất nhỏ có cơ hội đổi mới, sáng tạo trên cùng nền tảng như các doanh nghiệp lớn.

Tuy nhiên, bên cạnh những lợi ích rất lớn đối với cá nhân, xã hội và doanh nghiệp do các cuộc cách mạng số mang lại thì hành động phá hoại, trộm cắp và chia rẽ đến gián điệp và cố tình phá hoại cũng tự nhiên tồn tại trong môi trường kỹ thuật số mới.

Tội phạm mạng tương tự như các loại tội phạm khác, đều có thủ phạm và nạn nhân. Để thực hiện hành vi phạm tội chúng cần có động cơ, cơ hội và phương tiện. Khi công nghệ ngày càng phổ biến và ngày càng được sử dụng nhiều trong các hoạt động hàng ngày của quốc gia, doanh nghiệp và cá nhân, thì ngày càng nhiều cơ hội cho tội phạm mạng hoạt động. Khi khả năng truy cập và kết nối dễ dàng hơn, phương tiện và cơ hội cho các hành vi phạm tội mạng cũng tăng lên. Trước thời đại Internet, rất ít người biết cách sử dụng máy tính và có rất ít lý do để "tấn công" chúng. Ngày nay, có thể dễ dàng truy cập Internet từ thiết bị di động thông minh, nên phương tiện và cơ hội cũng từ đó tăng lên đáng kể. Hiện nay mọi người đều được kết nối với nhau và có nhiều cách sử dụng không gian ảo phục vụ cả mục đích cá nhân và thương mại, cả mục đích tốt và xấu.

1.1.1. Khái quát về tấn công, xâm nhập

Tất cả các hình thức truy cập vào một hệ thống máy tính, website, cơ sở dữ liệu, hạ tầng mạng, thiết bị của một cá nhân hoặc tổ chức thông qua mạng Internet với những mục đích nhất định được coi là xâm nhập mạng.

Khái niệm tấn công mạng (*hoặc "tấn công không gian mạng"*) trong tiếng Anh là Cyber attack (hoặc *Cyberattack*), được ghép bởi 2 từ: Cyber (thuộc không gian mạng internet) và *attack* (sự tấn công, phá hoại). Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.[2]

1.1.2. Các dạng tấn công, xâm nhập mạng

Tấn công mạng là quá trình xâm nhập trái phép vào hệ thống mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử nhằm chiếm được mật khẩu, dữ liệu, quyền truy cập hệ thống thông tin từ đó kẻ tấn công có thể khai thác thông tin sử dụng vào mục đích trái phép.[3] Điều này có thể gây ra cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động chủ sở hữu của hệ thống mạng khiến họ mất thời gian, nguồn lực và tiền bạc. Và không ai an toàn 100% trước các cuộc tấn công mạng.

Tấn công mạng chủ yếu qua các phương thức phổ biến sau:

1.1.2.1. Tấn công từ chối dịch vụ - DOS

Tấn công từ chối dịch vụ là một hành động tấn công khiến server hoặc tài nguyên mạng không khả dụng với người dùng, thông thường là làm gián đoạn tạm thời dịch vụ của một host kết nối Internet.

1.1.2.2. Từ chối dịch vụ phân tán – DDOS

DDOS là một phương pháp tấn công đến server bằng cách sử dụng nhiều thiết bị, máy tính khác nhau để đánh sập server. Hiện tượng tấn công DDOS là khi có rất nhiều truy cập vào cùng 1 lúc, làm cho dịch vụ bị gián đoạn, không sử dụng được server. Đối tượng tấn công DDOS không chỉ sử dụng máy tính của mình để tấn công, mà chính máy tính của người dùng cũng có thể đang được sử dụng để tấn công. Điểm khác biệt lớn nhất giữa DOS và DDOS là thay vì gửi request trực tiếp từ máy mình, hacker sẽ sử dụng các máy đã bị hack từ trước để đồng loạt gửi lượng lớn request và yêu cầu truy cập tới máy chủ.

1.1.2.3. Tấn công thông qua thu thập gói tin - Sniffing Attack

Thu thập gói tin là quá trình theo dõi và nắm bắt tất cả các gói dữ liệu đang đi qua một mạng máy tính. Các gói tin đánh giá (*packet sniffers*) được sử dụng để theo dõi lưu lượng dữ liệu đi qua mạng. Chúng được gọi là bộ phân tích giao thức mạng. Những kẻ tấn công sử dụng các công cụ đánh giá gói này để nắm bắt các gói dữ liệu trong mạng. Có nhiều loại công cụ

dò tìm khác nhau được sử dụng và chúng bao gồm Wireshark ,Ettercap , Better CAP, Tcpdump,WinDump , v.v.

1.1.2.4. Tấn công rà quét cổng dịch vụ, dò tìm lỗ hổng

Là hình thức tấn công nhằm thu thập các thông tin về hệ thống mục tiêu, từ đó phát hiện ra các điểm yếu. Cách thức mà kẻ tấn công tiến hành như sau: đầu tiên dùng kỹ thuật ping để kiểm tra xem hệ thống nạn nhân đang có những địa chỉ IP nào đang hoạt động. Sau đó kẻ tấn công sẽ kiểm tra những dịch vụ đang chạy, những cổng đang mở trên những địa chỉ IP tìm thấy ở trên. Công cụ mà kẻ tấn công thường sử dụng ở bước này là Nmap.

1.1.2.5. Tấn công vào tài khoản, mật khẩu

Tấn công vào tài khoản, mật khẩu hay Tấn công brute force là một trong những phương pháp hack đơn giản và ít phức tạp nhất. Đây là kiểu tấn công thủ công và không có nhiều kĩ thuật phức tạp: thử đoán mật khẩu vô số lần để tìm ra mật khẩu đung. Kẻ tấn công cố gắng giành quyền truy cập vào tài khoản người dùng bằng cách đoán tên username/email và mật khẩu. Thông thường, động cơ đằng sau brute force attack là sử dụng tài khoản bị vi phạm để thực hiện một cuộc tấn công quy mô lớn, đánh cắp dữ liệu nhạy cảm, tắt hệ thống hoặc kết hợp cả ba yếu tố này với nhau.

1.1.2.6. Tấn công thông qua giả mạo - Spoofing Attack

Khi thu thập, kẻ tấn công quan sát lưu lượng dữ liệu của mạng và bắt các gói dữ liệu bằng cách sử dụng trình đánh giá gói. Kẻ tấn công sẽ giả mạo đánh cắp thông tin đăng nhập của người dùng để khai thác với tư cách là người dùng hợp pháp.

- Giả mạo địa chỉ IP
- Giả mạo giao thức ARP
- Giả mạo giới thiệu
- Giả mạo địa lý

1.1.2.7. Tấn công chiếm quyền điều khiển phiên hoạt động - Session Hijacking

Tấn công phiên là quá trình chiếm lấy một phiên (*session*) đang hoạt động, mục đích nhằm vượt qua quá trình chứng thực truy cập không hợp lệ vào dịch vụ của một hệ thống máy tính.

Có 4 phương pháp chính được sử dụng tấn công chiếm phiên hoạt động là:

- Cố định phiên
- Chiếm phiên thông qua gói tin
- Chiếm phiên thông qua kịch bản
- Chiếm phiên thông qua quyền điều khiển trình duyệt

1.1.2.8. Tấn công qua lỗi tràn bộ nhớ đệm - Buffer Overflow Attack

Tấn công thông qua lỗi tràn bộ nhớ đệm là khi kẻ xâm nhập cung cấp các biên đầu vào hay dữ liệu vượt quá khả năng xử lý của chương trình làm cho hệ thống bị treo dẫn đến từ chối dịch vụ, từ đó kẻ xâm nhập sẽ lợi dụng chèn các thực thi trái phép nhằm thực hiện các đoạn mã nguy hiểm từ xa. Đa phần các lỗi tràn bộ nhớ đệm dẫn đến việc chiếm quyền điều khiển toàn bộ trên hệ thống nên đây là một kiểu tấn công thường được sử dụng. Tràn bộ nhớ đệm xảy ra trên nhiều hệ điều hành, đặc biệt là trên UNIX và Windows, và trên nhiều ứng dụng khác nhau như web, mail, ftp, dns, telnet, ssh, database, …

1.1.3. Các dạng tấn công, xâm nhập host

Tấn công xâm nhập host là cuộc tấn công nhắm mục tiêu vào một hệ thống hoặc máy chủ cụ thể ví dụ: máy tính xách tay, máy tính để bàn, điện thoại thông minh, v.v. Theo thống kê trong năm 2020, thế giới có tới 57% các cuộc tấn công vào máy chủ là vi rút, 21% là trojan và 2% là sâu, cùng với những loại khác trong đó có 5,6 tỷ tấn công bằng phần mềm độc hại, 304,6 triệu cuộc tấn công ransomware, 56,9 triệu cuộc tấn công phần mềm độc hại IoT, 81,9 triệu Các cuộc tấn công Cryptojacking, 3,8 triệu mối đe dọa mã hóa. [9]

1.1.3.1. Tấn công qua phần mềm độc hại - Self Propagating Programs

Đây là phương thức tấn công xâm nhập máy chủ phổ biến nhất.

Các phần mềm độc hại (*Self-Propagating Programs*) chủ yếu bao gồm [4][6]:

- Vi rút.
- Sâu.
- Trojans.
- Hybrids và Các hình thức khác.
- Ransomware.
- Phần mềm độc hại không cần tệp.
- Phần mềm quảng cáo.
- Phần mềm gián điệp.
- Bots và Botnets.
- Rootkits.

1.1.3.2. Tấn công khai thác các lỗ hổng hệ điều hành, phần mềm

Tấn công khai thác các lỗ hổng hệ điều hành, phần mềm là lợi dụng những lỗi hoặc điểm yếu trên hệ điều hành hay phần mềm của máy tính, thiết bị router, modem hoặc trong các ứng

dụng được cài đặt để khai thác (*exploit*) tài nguyên phục vụ cho mục đích vi phạm các chính sách bảo mật.

1.2. Tổng quan về phát hiện xâm nhập

Cùng với sự phát triển ngày càng lớn của hệ thống thông tin trên nền tảng kết nối toàn cầu, kẻ xâm nhập cũng phát triển qua nhiều phương thức và che giấu tinh vi hơn khiến người dùng mạng hay các phương tiện CNTT rất khó có thể tự phát hiện. Các hệ thống mạng, máy chủ cần phát hiện lỗ hổng khai thác xâm nhập và sự xâm nhập trước khi kẻ tấn công tác động ảnh hưởng đến hệ thống.

1.2.1. Khái quát về phát hiện xâm nhập

Phát hiện xâm nhập là quá trình giám sát các sự kiện (biểu hiện) xuất hiện trong một hệ thống mạng hoặc trên một máy tính và phân tích các dấu hiệu có thể là sự xâm phạm hoặc mối đe dọa sắp xảy ra xâm phạm các chính sách an toàn an ninh hoặc các chuẩn an toàn của mạng hoặc máy tính .[3]

Phát hiện xâm nhập còn là khả năng nhận dạng xâm nhập do các cá nhân gây ra, bao gồm: những người sử dụng hệ thống bất hợp pháp *("tội phạm máy tính" - hacker)* và những người sử dụng hợp pháp nhưng lại lạm dụng các đặc quyền của mình "đe doạ bên trong" nhằm phá vỡ đến tính toàn vẹn, tính sẵn sàng, tính tin cậy của các cơ chế bảo mật hệ thống mạng hoặc máy chủ.

1.2.2. Phát hiện xâm nhập mạng và phát hiện xâm nhập host

Hệ thống IDS dựa theo kiểu phạm vi giám sát được phân làm 2 loại là: Phát hiện xâm nhập mạng và phát hiện xâm nhập host.[3]

1.2.2.1. Phát hiện xâm nhập mạng (NIDS - Network -based IDS)

NIDS thường được đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau firewall trong các hệ thống mạng để giám sát gói tin trao đổi giữa các thiết bị. Hệ thống này sẽ quét tất cả thông tin ra - vào của hệ thống. NIDS cung cấp dữ liệu về hiệu suất mạng nội bộ, tổng hợp lại các gói tin và phân tích chúng.

1.2.2.2. Phát hiện xâm nhập host (HIDS – Host -based IDS)

Những hệ thống Host-based là kiểu IDS được nghiên cứu và triển khai đầu tiên. Bằng cách cài đặt những phần mềm IDS trên các máy trạm *(gọi là Agent),* HIDS có thể giám sát toàn bộ hoạt động của hệ thống, các log file và lưu thông mạng đi tới từng máy trạm. IDS kiểm tra lưu thông mạng đang được chuyển đến máy trạm, bảo vệ máy trạm thông qua việc ngăn chặn các gói tin nghi ngờ. HIDS có khả năng kiểm tra hoạt động đăng nhập vào máy trạm, tìm

kiếm các hoạt động không bình thường như dò tìm mật khẩu, leo thang đặc quyền. Ngoài ra HIDS còn có thể giám sát sâu vào bên trong Hệ điều hành của máy trạm để kiểm tra tính toàn vẹn của nhân hệ điều hành, file lưu trữ trong hệ thống.

1.2.3. Phát hiện xâm nhập dựa trên dấu hiệu và dựa trên bất thường

Hệ thống IDS dựa theo các triển khai kỹ thuật thực hiện được phân làm 2 loại là: Phát hiện xâm nhập dựa trên dấu hiệu và dựa trên bất thường.

1.2.3.1. Phát hiện xâm nhập dựa trên dấu hiệu

Phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập (*Signature-based IDS*) thông qua phân tích lưu lượng mạng và nhật ký hệ thống. Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập (*signature database*), và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới.

1.2.3.2. Phát hiện xâm nhập dựa trên bất thường

Phát hiện dựa trên bất thường (*Anomaly-based IDS)* là quá trình so sánh các định nghĩa của hoạt động được xem xét bình thường so với sự kiện quan sát được để xác định các sai lệch quan trọng. Thường là cách so sánh các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (*anomaly*) có thể là dấu hiệu của xâm nhập.

1.3. Kết luận Chương I

Chương này cung cấp một cái nhìn tổng quan về xâm nhập và phát hiện xâm nhập. Qua đó biết được mục đích và tác hại của tấn công xâm nhập và giới thiệu các hệ thống phát hiện xâm nhập phân tích các dấu hiệu của sự xâm nhập hoặc mối đe dọa sắp xảy ra đến các chính sách an toàn máy tính, hoặc các chuẩn an toàn.

Từ đó có phân loại các hệ thống phát hiện xâm nhập theo kiểu phạm vi giám sát và theo các kiểu triển khai kỹ thuật thực hiện.

CHƯƠNG II. CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP

Trong chương này sẽ cho chúng ta cái nhìn tổng quan về IDS bao gồm cả những điểm mạnh và điểm yếu của chúng. Chúng ta sẽ đề cập đến cả Network IDS và cả Host IDS. Sự khác nhau chủ yếu giữa NIDS và HIDS đó là dữ liệu mà nó tìm kiếm. Bên cạnh đó chương này cũng tìm hiểu một số hệ thống phát hiện xâm nhập tiêu biểu như: Snort, Suricata, OSSEC, SolarWinds Security Event Manager, IBM Qradar, Security Onion.

2.1. Các hệ thống phát hiện xâm nhập mạng

Các hệ thống phát hiện xâm nhập mạng sẽ theo dõi lưu lượng và phân tích các gói tin truyền trong mạng của hệ thống. Snort và Suricata là hai hệ thống phát hiện xâm nhập mạng có các thành phần và tính năng nổi bật.

2.1.1. Snort

2.1.1.1. Snort là gì?

Snort là một hệ thống mã nguồn mở phát hiện và ngăn chặn xâm nhập mạng miễn phí. Nó sử dụng ngôn ngữ dựa trên quy tắc, thực hiện phân tích giao thức, tìm kiếm kết hợp nội dung và có thể được sử dụng để phát hiện nhiều loại tấn công và thăm dò khác nhau, chẳng hạn như buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts ….[7]

2.1.1.2. Thành phần và chức năng

Snort có 5 thành phần chính như sau:

- Bộ giải mã gói tin - Packet Decoder.
- Các bộ tiền xử lý – PreProcessers
- Máy phát hiện - Detection Engine
- Hệ thống cảnh báo và nhật ký - Logging and Alerting System
- Môđun xuất - Output Modules

Bộ phận đầu ra của Snort phụ thuộc vào việc ta ghi các ghi nhận, thông báo theo cách thức nào. Có thể cấu hình bộ phận này để thực hiện các chức năng sau:

- Lưu các ghi nhận và thông báo theo định dạng file văn bản hoặc cơ sở dữ liệu.
- Gửi thông tin SNMP.
- Gửi các thông điệp đến hệ thống ghi log.
- Lưu các ghi nhận và thông báo vào cơ sở dữ liệu *(MySQL, Oracle...).*
- Chỉnh sửa cấu hình trên Router, Firewall.

Snort có 4 chế độ hoạt động như sau:

- Chế độ đánh giá gói tin - Sniffer mode: ở chế độ này Snort sẽ đánh giá và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị.

- Chế độ lưu nhật ký gói tin - Packet Logger mode: lưu trữ các gói tin trong các tập tin log.

- Chế độ phát hiện xâm nhập mạng - Network instruction detect system (NIDS): đây là chế độ hoạt động mạnh mẽ và được áp dụng nhiều nhất, khi hoạt động ở chế độ NIDS Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với các thông tin được định nghĩa của người dùng để từ đó có những hành động tương ứng.

- Chế độ nội tuyến - Inline mode: khi triển khai Snort trên Linux thì chúng ta có thể cấu hình Snort để phân tích các gói tin từ các bảng IP (*iptables*) thay vì thư viện ảnh chụp gói (*libpcap*) do đó iptable có thể thông qua các gói tin theo luật Snort.

*2.1.1.3. **Ưu nhược điểm của Snort***

a. Ưu điểm

- Snort là phần mềm mã nguồn mở, hoạt động 24/7 theo thời gian thật.

- Chạy trên nhiều nền tảng khác nhau: Không chỉ chạy trên các hệ điều hành nguồn mở như GNU/Linux mà Snort còn có thể chạy được trên các nền tảng thương mại như Microsoft Windows, Solaris, HP-UX...

- Các luật của Snort thường xuyên được bổ sung và cập nhật các hình thức xâm nhập mới.

- Có khả năng phát hiện một số lượng lớn các kiểu thăm dò, xâm nhập khác nhau như: buffer oveflow, CGI-Atack, Scan, ICMP, Virus...

- Có một cộng đồng của người sử dụng và các nhà phát triển.

- Có rất nhiều add-on mà không phải là thành phần của Snort, nhưng cung cấp thêm các tính năng và dễ sử dụng.

- Snort không cần phải thay thế bất kỳ cơ sở hạ tầng an ninh hiện có.

b. Nhược điểm

- Có thể xảy ra trường hợp báo động giả, tức là không có dấu hiệu bất thường mà IDS vẫn báo (*False Positive*).

- Không phân tích được các lưu lượng được mã hóa như SSH, IPSec, SSL, v.v…

- NIDS đòi hỏi phải luôn được cập nhật các dấu hiệu tấn công mới nhất để thực sự hoạt động hiệu quả.

- Không thể cho biết việc mạng bị tấn công có thành công hay không.

- Một trong những hạn chế là giới hạn băng thông. Những bộ thu thập dữ liệu phải thu thập tất cả lưu lượng mạng, sắp xếp lại và phân tích chúng. Khi tốc độ mạng tăng lên thì khả năng của bộ thu thập thông tin cũng vậy. Một giải pháp là phải đảm bảo cho mạng được thiết kế chính xác.

2.1.2. Suricata

2.1.2.1. Suricata là gì?

Suricata là một hệ thống phát hiện xâm nhập dựa trên mã nguồn mở. Nó được phát triển bởi *Open Information Security Foundation (OISF)*. Công cụ này được phát triển không nhằm cạnh tranh hay thay thế các công cụ hiện có, nhưng nó mang lại những ý tưởng và công nghệ mới trong lĩnh vực an ninh mạng.

Suricata là công cụ IDS/IPS (*Intrusion Detection System / Intrusion Prevention System*) phát hiện và ngăn chặn xâm nhập dựa trên luật để theo dõi lưu lượng mạng và cung cấp cảnh báo đến người quản trị hệ thống khi có sự kiện đáng ngờ xảy ra. Nó được thiết kế để tương thích với các thành phần an ninh mạng hiện có. Bản phát hành đầu tiên chạy trên nền tảng linux 2.6 có hỗ trợ nội tuyến (*inline*) và cấu hình giám sát lưu lượng thụ động có khả năng xử lý lưu lượng lên đến gigabit. Suricata là công cụ IDS/IPS miễn phí trong khi nó vẫn cung cấp những lựa chọn khả năng mở rộng cho các kiến trúc an ninh mạng phức tạp nhất.

2.1.2.2. Thành phần và chức năng của Suricata

Suricata được phát triển dựa trên Snort nên nó vẫn giữ nguyên kiến trúc bên trong của Snort. Kiến trúc của nó có nhiều thành phần, với mỗi thành phần có một chức năng riêng.

Kiến trúc của Suricata gồm 4 phần cơ bản sau:

a. Đánh giá và giải mã gói tin - The Sniffer (*Packet Decoder*).

b. Phân tích dữ liệu - The Preprocessors. [6]

c. Máy phát hiện - The Detection Engine.

Các luật có thể được chia thành 2 phần:

Phần Hearder***:*** gồm các hành động (*log/ alert*), loại giao thức (*TCP, UDP, ICMP...),* địa chỉ IP nguồn, địa chỉ IP đích và port.

Phần Options: là phần nội dung của gói tin được tạo ra để phù hợp với luật.

Luật là phần quan trọng mà bất cứ ai tìm hiểu về Suricata cần phải nắm rõ.

d. Xuất kết quả - The Output gồm hai modules:

Modul Alert/ Logging

Modul kết xuất thông tin

2.1.2.3. Ưu nhược điểm của Suricata

a. Ưu điểm

- Dễ dàng cấu hình: Suricata làm việc như thế nào, tập tin cấu hình ở đâu, các luật như thế nào người quản trị đều có thể biết và cấu hình theo ý mình được.

- Suricata là phần mềm mã nguồn mở: Sricata được phát hành dưới giấy phép GNU/GPL điều này có nghĩa là bất cứ ai cũng có thể sử dụng Suricata một cách miễn phí dù đó là doanh nghiệp hay người dùng cá nhân. Ngoài ra vì là phần mềm mã nguồn mở nên Suricata có một cộng đồng người sử dụng lớn.

- Chạy trên nhiều nền tảng khác nhau: Chạy trên các hệ điều hành nguồn mở như Linux, CentOS. Debian, Fedora, FreeBSD, Window, Mac OS X…

- Luật của Suricata thường xuyên được cập nhật: Các luật của Suricata thường xuyên được bổ sung và cập nhật các hình thức xâm nhập mới.

b. Nhược điểm

- Việc kiểm tra nội dung của mọi gói mạng là cực kỳ tốn CPU, đặc biệt là đối với tải lưu lượng nhiều gigabit. Và đây thường là yếu tố hạn chế trong hiệu suất Suricata: xử lý gói tin trên CPU.

2.2. Các hệ thống phát hiện xâm nhập host

Các hệ thống phát hiện xâm nhập host sẽ theo dõi lưu lượng và phân tích log trên các client được liên kết đến hệ thống. OSSEC và Suricata là hai hệ thống phát hiện xâm nhập host tiêu biểu.

2.2.1. OSSEC

2.2.1.1. OSSEC là gì?

OSSEC là phần mềm mã nguồn mở giúp phát hiện xâm nhập dựa trên host (*HIDS*) . OSSEC dựa trên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau. OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường. Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC. OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra. Các hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC. Ngoài việc được triển khai như một HIDS, nó thường được sử dụng như một công cụ phân tích log, theo dõi và phân tích các bản ghi lại, IDS, các máy chủ Web và

các bản ghi xác thực. OSSEC chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris và Microsoft Windows.[11]

2.2.1.2. Thành phần và chức năng

Các thành phần và chức năng chủ yếu của OSSEC là:

Log based Intrusion Detection (*LIDs*) and Log Monitoring:

Rootkit and Malware Detection:

File Integrity Monitoring (*FIM*):

Phát hiện các thay đổi đối với hệ thống.

Active Response:

System Inventory:

- Ossec thường hoạt động theo mô hình Server-Agent/Agentless có thể cài trên các môi trường OS sau:

+ Manager (*Server*) là nơi lưu trữ cơ sở dữ liệu của việc kiểm tra tính toàn vẹn file .Quản lý, lưu tất cả các rule, decoder (bộ giải mã), cấu hình chính.

+ Agent là 1 phần mềm được cài đặt trên máy client giúp thu thập các thông tin và gửi cho Server để phân tích, thống kê. Agent cung cấp một số thông tin được thu thập theo thời gian thực.

+ Agentless là các hệ thống không cài được gói Ossec-agent. Trên các Agentless này có thể thực hiện việc kiểm tra tính toàn vẹn, giúp monitor firewall, router hay thậm chí cả hệ thống Unix.

+ Ảo hóa/ VMware - Ossec cho phép cài đặt agent trên các guest OS (Máy ảo). Ossec cũng giám sát việc login, logouts và các lỗi bên trong ESX Server. Ngoài ra nó cũng cảnh báo nếu bất kỳ tùy chọn cấu hình không an toàn nào được bật.

+ Firewalls, switches and routers là thiết bị tương tự như các Agentless, Ossec có thể nhận và phân tích nhật ký hệ thống từ nhiều firewall, switch, router.

2.2.1.3. Ưu nhược điểm của Ossec

a. Ưu điểm

- Ossec hỗ trợ cài đặt đa nền tảng *(Linux, Mac OS, Window, Solaris).*

- Chức năng Cảnh báo thời gian thực *(Real-time Alert)* kết hợp với smtp, sms, syslog sẽ cho phép người dùng nhận cảnh báo trên các thiết bị có hỗ trợ email.

- Ngoài ra tính năng Active-respone có thể giúp block cuộc tấn công ngay lập tức.

- Có thể tích hợp với các hệ thống hiện đại (*SIM/SEM*)

- Mô hình Server – Agent/Agentless, cho phép Server dễ dàng quản lý tập trung các chính sách trên nhiều OS.

- Ossec hỗ trợ giám sát trên cả agent, agentless (*Client không cài đặt được gói agent*) như các thiết bị router, firewall.

b. Nhược điểm

- Khả năng nâng cấp của Ossec khá phức tạp và tương đối khó khăn. Các quy tắc cũ sẽ bị xóa hoặc bị quy tắc mới ghi đè sau khi nâng cấp hệ thống.

2.2.2. SolarWinds Security Event Manager

2.2.2.1. SolarWinds Security Event Manager là gì?

SolarWinds® Security Event Manager (*SEM*) là một phần mềm giải pháp giám sát phát hiện xâm nhập host được pháy triển bởi công ty SolarWinds Inc. SolarWinds SEM thu thập dữ liệu nhật ký trong hệ thống mạng từ hai tài nguyên: Thiết bị Agents - là một ứng dụng phần mềm thu thập và chuẩn hóa dữ liệu nhật ký trước khi nó được gửi đến Trình quản lý SEM và các thiết bị Non Agent - những thiết bị gửi dữ liệu nhật ký trực tiếp đến Trình quản lý SEM để chuẩn hóa và xử lý.

Sau khi chuẩn hóa, Trình quản lý SEM xử lý dữ liệu rồi so sánh tương quan dữ liệu dựa trên các quy tắc do người dùng xác định và bộ lọc cảnh báo cục bộ, đồng thời bắt đầu các hành động liên quan khi có thể. [8]

2.2.2.2. Thành phần và chức năng

Một cài đặt SEM hoàn chỉnh bao gồm các thành phần sau:

- Trình quản lý SEM (hoặc SEM VM), thu thập và xử lý thông tin nhật ký và sự kiện. Thành phần này được cài đặt đầu tiên.

- Phần mềm máy tính để bàn hoặc ứng dụng web cho phép xem thông tin SEM từ máy tính để bàn hoặc máy tính xách tay.

Trình quản lý SEM là trang điều khiển tổng quát của một thiết bị dựa trên Linux. Trình quản lý SEM thu thập và xử lý thông tin nhật ký và sự kiện. Nó bao gồm các hệ thống nhân Linux được tùy biến lại kết hợp với các và dịch vụ máy chủ Syslog và máy thu bẫy SNMP. Dữ liệu thông tin được nén và tối ưu hóa cho tìm kiếm tại máy chủ web thông qua các cơ chế so sánh tương quan

SEM chấp nhận đầu vào của thiết bị bằng giao thức TCP và UDP. SEM Agent được cài đặt trên máy trạm, máy chủ và các thiết bị mạng khác. Nó thu thập và chuẩn hóa dữ liệu nhật ký trong thời gian thực như Nhật ký sự kiện Windows, nhiều loại nhật ký cơ sở dữ liệu và

nhật ký cục bộ trên mỗi thiết bị và truyền dữ liệu đó qua TCP tới Trình quản lý SEM. Nhật ký hệ thống truyền thông điệp qua TCP tới Trình quản lý SEM. TCP được ưu tiên hơn UDP vì TCP đảm bảo các thông điệp đến được nguyên vẹn.

2.2.2.3. Ưu nhược điểm của SolarWinds Security Event Manager

a. Ưu điểm

- Một trong những tính năng đáng giá nhất của SolarWinds SEM là cho phép thu thập nhật ký từ hầu hết mọi nguồn dữ liệu, sử dụng nhiều loại xác thực và thu thập và khả năng chuẩn hóa nhật ký từ các hệ thống khác nhau thành một định dạng chung.

- So với các hệ thống khác, SolarWinds SEM tương đối dễ dàng để thiết lập chạy và sử dụng, các thiết bị ảo cũng rất dễ bảo trì.

- SolarWinds SEM cho phép tùy chỉnh trang tổng quan mỗi người dùng để có thể nhanh chóng tìm thấy thông tin liên quan đến vị trí của mình.

b. Nhược điểm

- Mặc dù thiết lập ban đầu khá đơn giản, nhưng các tùy chỉnh đối báo cáo để định cấu hình chính xác các cảnh báo thích hợp lại tương đối phức tạp.

- Tính năng cảnh báo qua email với SolarWinds sẽ gửi một số lượng lớn email cảnh báo trùng lặp.

2.3. Các hệ thống phát hiện xâm nhập tích hợp

2.3.1. IBM Qradar

2.3.1.1. IBM Qradar là gì?

IBM QRadar là dòng sản phẩm được cung cấp bởi hệ điều hành bảo mật thông minh độc quyền của IBM - SIOS. Danh sách sản phẩm bao gồm Trình quản lý lỗ hổng QRadar (QRadar Vulnerability Manager) để quét mạng và phát hiện lỗ hổng, Cố vấn QRadar với Watson (QRadar Advisor with Watson), Phân tích hành vi người dùng QRadar (QRadar User Behavior Analysis), Trình quản lý rủi ro QRadar (QRadar Risk Manager), Quản lý sự kiện và bảo mật thông tin Qradar (QRadar SIEM), và nhiều hơn thế nữa. Tất cả các sản phẩm này hoạt động trên một nền tảng chung đảm bảo việc dễ dàng tích hợp, khả năng mở rộng, cũng như đơn giản bằng cách cung cấp nhiều chức năng và sản phẩm trong trải nghiệm người dùng tổng thể. Bằng cách hợp nhất các sự kiện nhật ký và dữ liệu luồng mạng từ thiết bị, điểm cuối và ứng dụng được phân phối trên toàn mạng, QRadar thu thập tất cả các thông tin khác nhau này và tổng hợp các sự kiện liên quan thành các cảnh báo duy nhất để tăng tốc độ phân tích và khắc phục sự cố.[5]

2.3.1.2. Thành phần và chức năng

Các thành phần kiến trúc của giải pháp được mô tả dưới đây:

Bảng điều khiển QRadar - QRadar Console là một phần trung tâm của giải pháp cung cấp giao diện người dùng, thông tin tài sản, trang tổng quan, báo cáo, xâm nhập cũng như các chức năng quản trị. Nó hoạt động như một cơ sở dữ liệu tổng thể với các bản sao tùy chọn được triển khai trên Bộ xử lý sự kiện (EP) để sao lưu và khôi phục tự động. Bảng điều khiển nhận dữ liệu từ EP đi qua Bộ lọc tràn để đảm bảo rằng luồng dữ liệu đến đáp ứng các quy tắc. Các sự kiện tiếp theo đã được đánh dấu để điều tra thêm hoặc vi phạm được tạo ra sẽ được chuyển cho thành phần đánh giá (Magistrate). Các đánh giá sẽ dựa tương quan các sự kiện trên các bộ xử lý sự kiện (Event Processor). Các đánh giá này được chuyển thông qua Ariel Proxy Server, một phần của bảng điều khiển, thu thập thông tin từ Ariel Query.

Máy chủ Bộ xử lý sự kiện EP sẽ quản lý tất cả các sự kiện và luồng đã kích hoạt việc tạo ra hành vi phạm tội. Công cụ phát hiện dị thường (ADE) cũng là một phần của bảng điều khiển, nó tìm kiếm mô-đun tích lũy trên Bộ xử lý sự kiện để tìm các điểm bất thường có thể xảy ra. ADE sử dụng ba loại quy tắc:

- Quy tắc ngưỡng - kiểm tra phạm vi số chẳng hạn như truyền dữ liệu đi lớn.

- Sự bất thường - thay đổi trong hành vi so với khung thời gian dài hơn, tức là hoạt động dịch vụ mới.

- Hành vi - sự khác biệt so với cùng một thời điểm trong ngày hoặc tuần trước đó, tức là các vấn đề về quy trình sao lưu.

Cuối cùng, Máy chủ quản lý thông tin lỗ hổng bảo mật chịu trách nhiệm duy trì tài sản, cơ sở dữ liệu.

Bộ xử lý sự kiện - Event Processor.

Bộ thu thập sự kiện - Event Collector.

Bộ thu thập luồng - Flow Collector

- So sánh chữ ký - so sánh chuỗi trong tải trọng, hỗ trợ cả chữ ký tùy chỉnh

- So sánh dựa trên cổng - tức là cổng 443 được xác định là HTTPS.

Có hai thành phần tùy chọn khác trong kiến trúc SIEM: Nút dữ liệu QRadar (QRadar Data Node) và Máy chủ ứng dụng QRadar (QRadar App Host). Nút dữ liệu cung cấp khả năng lưu trữ và xử lý cho việc triển khai QRadar. Máy chủ ứng dụng là máy chủ được quản lý chuyên dụng cung cấp tài nguyên CPU và bộ nhớ để chạy các ứng dụng.

IBM Security App Exchange.

QRadar Phân tích hành vi người dùng (QRadar User Behaviour Analytics UBA).

2.3.1.3. Ưu nhược điểm của IBM Qradar

a. Ưu điểm

- Giải pháp của IBM hỗ trợ các tùy chọn triển khai Tính khả dụng cao (Hight Availability-HA) cho cả thiết bị vật lý và thiết bị ảo với phương pháp tiếp cận máy chủ chính và phụ được kết hợp thành một cụm, trong đó máy chủ phụ ở trạng thái chờ và trong trường hợp máy chủ chính bị lỗi sẽ đảm nhận chức năng triển khai.

- IBM QRadar có khả năng lưu trữ nhiều người thuê trong một lần triển khai. Miền được tạo cho mỗi người thuê liên kết các nguồn dữ liệu với chúng và cách ly môi trường của người thuê với nhau.

- IBM cung cấp tài liệu đặc biệt cho từng khía cạnh của sản phẩm, đây là một lợi thế lớn để hiểu giải pháp, triển khai và quản trị nó.

b. Nhược điểm

- Đối với người sử dụng, QRadar có kiến trúc hơi phức tạp khiến việc quản lý tất cả các bộ phận trong cấu trúc tương đối khó khăn.

- Các yêu cầu cấu hình máy đáp ứng đối với hệ thống là khá cao.

2.3.2. Security Onion

Doug Burks bắt đầu xây dựng Security Onion dựa trên một dự án mở và miễn phí vào năm 2008 để cung cấp một nền tảng toàn diện để phát hiện xâm nhập, giám sát an ninh mạng và quản lý nhật ký. Vào năm 2014, Security Onion Solutions, LLC chính thức được thành lập. Security Onion được phân phối và duy trì bởi Security Onion Solutions, LLC.[10]

2.3.2.1. Security Onion là gì?

Security Onion là một bản phân phối Linux miễn phí và mở để tìm kiếm mối đe dọa, giám sát an ninh doanh nghiệp và quản lý nhật ký. Nó bao gồm TheHive , Playbook và Sigma, Fleet và osquery , CyberChef , Elasticsearch , Logstash , Kibana , Suricata , Zeek , Wazuh và nhiều công cụ bảo mật khác. Các chương trình này tồn tại và được phát triển như các giải pháp hoạt động độc lập. Nhưng vì mục đích chuyên biệt cao, không phải tất cả các bản phân phối Linux đều được tích hợp những công cụ trên. Và, việc cài đặt tất cả công cụ từ nhiều mã nguồn khác nhau khá khó khăn. Security Onion đã giải quyết vấn đề này rất hiệu quả và thành công. Security Onion có công cụ để cung cấp cho vấn đề bảo mật hệ thống mạng và máy chủ. Security Onion có thể được sử dụng làm Hệ thống phát hiện xâm nhập (IDS) kết hợp NIDS

và HIDS. Người dùng chỉ cần thông qua các bước cài đặt một hệ thống duy nhất, sau đó đã có thể sử dụng tất cả các công cụ được tích hợp sẵn trong Security Onion.[10]

Security Onion thường được sử dụng để theo dõi lưu lượng truy cập từ phía trong và ngoài hệ thống nhằm phát hiện các xâm nhập vào môi trường, thiết lập lệnh và kiểm soát hoặc có thể là xâm nhập dữ liệu. Security Onion có thể sử dụng nhật ký từ các máy chủ và máy trạm trong hệ thống để sau đó người quản trị có thể tìm kiếm trên tất cả các mạng và nhật ký lưu trữ cùng một lúc.

2.3.2.2. Thành phần và chức năng

Security Onion kết hợp liền mạch ba chức năng chính là:

- Chụp toàn bộ gói tin trong hệ thống.
- Phát hiện mạng và điểm cuối trong hệ thống.
- Công cụ phân tích mạnh mẽ.

Chụp toàn bộ gói tin

Phát hiện mạng và điểm cuối.

- Phát hiện xâm nhập mạng - NIDS.
- Siêu dữ liệu giao thức - Protocol metadata.
- Phát hiện xâm nhập host – HIDS

Các công cụ phân tích - Analysis Tools. Hiện Security Onion đã tích hợp chặt chẽ các công cụ sau:

- Security Onion Console (SOC).
- TheHive.
- Kibana).
- CyberChef.
- Playbook.

2.3.2.3. Ưu nhược điểm của Security Onion

a. Ưu điểm

- Security Onion là một phần mềm hoàn toàn miễn phí sử dụng nhân hệ điều hành mã nguồn mở Linux với một cộng đồng hỗ trợ lớn.
- Security Onion tích hợp một loạt công cụ bảo mật linh hoạt cao bao gồm các công cụ quản lý cảm biến, bộ phân tích lưu lượng và bộ dò tìm gói tin được cài đặt sẵn và có thể được vận hành mà không cần bất kỳ phần mềm IDS / IPS bổ sung nào.
- Security Onion được cập nhật thường xuyên để cải thiện mức độ bảo mật.

b. Nhược điểm

Ngoài những ưu điểm trên Security Onion vẫn còn tồn tại một vài điểm yếu sau:

- Security Onion chưa hỗ trợ Wi-Fi để quản lý mạng.

- Quản trị viên cần bổ sung kiến thức để tìm hiểu các công cụ khác nhau để sử dụng hiệu quả bản phân phối Security Onion.

- Không có sao lưu tự động các tệp cấu hình ngoại trừ các quy tắc. Để sao lưu được người dùng cần sử dụng phần mềm của bên thứ ba.

2.4. Phân tích so sánh các hệ thống phát hiện xâm nhập

IDS là một công nghệ bảo mật được tạo ra nhằm xác định và cô lập các hành vi xâm nhập hệ thống máy tính. Mỗi hệ thống IDS khác nhau sẽ có cách tiếp cận khác nhau. Do đó các chuyên gia bảo mật cần lựa chọn IDS phù hợp cho hệ thống máy tính cụ thể của mình. Điều này khá phức tạp bởi hiện tại đang có vô số các giải pháp trên thị trường. Các tiêu chí, đặc tính sẽ được lựa chọn, xác định để so sánh và đánh giá các cách giải pháp khác nhau.

2.5. Kết luận Chương II

Chương này đã liệt kê một số công cụ phát hiện xâm nhập tiêu biểu của các loại mô hình hệ thống phát hiện xâm nhập mạng, host và hệ thống phát hiện xâm nhập tích hợp. Qua đó phân tích công nghệ, các thành phần và chức năng của mỗi công cụ. Cuối cùng là so sánh ưu, nhược điểm của các công cụ cũng như từng mô hình hệ thống phát hiện xâm nhập.

CHƯƠNG III. THỬ NGHIỆM TRIỂN KHAI GIẢI PHÁP PHÁT HIỆN XÂM NHẬP TÍCH HỢP SECURITY ONION CHO MẠNG LAN

Chương III sẽ đi sâu vào một giải pháp phát hiện xâm nhập tích hợp tiêu biểu là Security Onion. Trong chương mô tả các bước triển khai thành phần một hệ thống Security Onion cơ bản và các kịch bản tấn công thử nghiệm, từ đó đánh giá kết quả đạt được.

3.1. Mô hình triển khai

3.1.1. Sơ đồ triển khai hệ thống Security Onion cho bảo mật mạng LAN

Sơ đồ triển khai Security Onion cơ bản gồm 3 thành phần chính:

- Hệ thống mạng bao gồm Internet, firewall, router, switch: là nơi Security Onion lắng nghe các cuộc tấn công từ các cổng của bộ chuyển mạch.

- Hệ thống Security Onion: là thành phần chính của sơ đồ được đặt sau lớp mạng.

- Hệ thống máy chủ: gồm các máy chủ hoặc máy người dùng trong hệ thống mạng.

3.1.2. Các yêu cầu phần cứng và phần mềm

3.1.2.1. Yêu cầu phần cứng

Security Onion chỉ hỗ trợ kiến trúc x86-64. Để cài đặt Security Onion yêu cầu hệ thống tối thiểu là CPU 4 Cores và RAM 8GB.

3.1.2.2. Yêu cầu phần mềm

Để cài đặt Security Onion, cần tải xuống file ISO Security Onion hoặc tải xuống file ISO Ubuntu 16.x tiêu chuẩn rồi thêm PPA Security Onion và các gói thành phần.

3.2. Triển khai Security Onion cho mạng LAN

Các bước cài đặt hệ thống Security Onion

3.2.1. Triển khai thành phần phát hiện xâm nhập mạng – NIDS

Sau khi hoàn thành cài đặt Security Onion thì hệ thống đã được chạy như IDS. Security Onion có thể chạy Snort hoặc Suricata làm Hệ thống phát hiện xâm nhập mạng (NIDS).

3.2.2. Triển khai thành phần phát hiện xâm nhập host – HIDS

Ngoài các thành phần phát hiện xâm nhập mạng, Security Onion cũng có thể thu thập nhật ký từ các điểm cuối. Security Onion sử dụng Beat,OSSEC/ Wazuh và Sysmon làm thành phần phát hiện xâm nhập host (HIDS).

3.2.3. Triển khai thành phần giao diện và quản trị

Security Onion sử dụng Elastic Stack để tổng hợp dữ liệu từ các thành phần hệ thống sau đó phân tích và hiển thị trực quan dữ liệu đó theo thời gian thực. Elastic Stack tích hợp cho Security Onion bao gồm các ngăn thành phần là Elasticsearch, Logstash và Kibana.

3.3. Một số kịch bản thử nghiệm, kết quả và đánh giá

3.3.1. Một số kịch bản thử nghiệm phát hiện tấn công, xâm nhập

Các kịch bản thử nghiệm phát hiện tấn công, xâm nhập vào hệ thống được xây dựng trên nền Oracle VM VirtualBox bao gồm máy chủ Security Onion phiên bản 16.04, máy tính client Windows 10, và máy tính tấn công Kali Linux.

3.3.1.1. Tấn công dò cổng

Kịch bản này kẻ xâm nhập sẽ sử dụng máy tính Kali Linux tiến hành dò tìm các cổng đang được mở trên máy tính Windows. Đối tượng sẽ sử dụng Nmap dò tìm trên địa chỉ 192.168.56.102 của máy tính Windows và nhận thấy các cổng 135/TCP của dịch vụ msrpc, cổng 138/TCP của dịch vụ netbios-ssn và cổng 445/TCP của dịch vụ microsoft-ds đang mở.

3.3.1.2. Tấn công Dos

Kịch bản này kẻ xâm nhập sẽ sử dụng Hping3 từ máy tính Kali Linux thực hiện tấn công Dos đến máy tính Windows. Ngoài ra đối tượng sẽ giả mạo địa chỉ tấn công là 192.168.56.104.

3.3.1.3. Tấn công giao thức FTP

Kịch bản này kẻ xâm nhập sẽ tiến hành quét các thông tin, mật khẩu đăng nhập của người dùng tại máy chủ FTP trên máy tính Windows.

3.3.1.4. Tấn công quét lỗ hổng Web Server

Kịch bản này kẻ tấn công sẽ quét để tìm các lỗ hổng nhằm xâm nhập hệ thống Webserver từ máy tính Kali Linux.

Sau khi biết được thông tin của trang web, đối tượng tiếp tục sử dụng công cụ Wpscan để tìm các lỗ hổng của máy chủ Web.

3.3.1.5. Khai thác lỗ hổng Eternalblue Windows

Kịch bản này kẻ xâm nhập sẽ quét và khai thác Eternalblue, lỗ hổng ms17-010 của Windows. Lỗ hổng này chính là nguyên nhân khiến WannaCry có thể lây lan mạnh mẽ. Đối tượng sẽ sử dụng công cụ Metasploit trên máy tính Linux để khai thác lỗ hổng này.

3.3.2. Các kết quả

Sau khi phát hiện các tình huống xâm nhập hệ thống, Sercurity Onion sẽ tổng hợp logs và chuyển qua một bộ phân tích chung sau đó xuất ra các cảnh báo. Người dùng sẽ sử dụng giao diện Kibana hoặc Squert được tích hợp sẵn trong gói cài đặt Sercurity Onion để có thể xem

chi tiết, thông kê phân tích hay xuất ra báo cáo. Giao diện chính của thành phần quản trị sẽ hiển thị tổng số lượng cảnh báo, biểu đồ phân bổ theo thời gian và các thông tin chính của cảnh báo.

Sau các cuộc tấn công ở trên, Security Onion đều phát hiện được tức thì và đưa ra cảnh báo realtime ngay trên giao diện quản trị. Trong lúc các cuộc tấn công diễn ra, Security Onion vẫn hoạt động tốt để duy trì sự ổn định của hệ thống mạng. Tuy nhiên, khi tấn công đồng thời nhiều phương thức khác nhau cùng một lúc, hệ thống thử nghiệm đã sử dụng CPU ở mức tối đa 90~100%, các gói tin đánh giá cũng phản hồi kết quả chậm hơn.

3.3.3. Nhận xét, đánh giá.

Security Onion chính là một bản phối miễn phí hoàn chỉnh tích hợp các công cụ để thu thập và phân tích dữ liệu hành vi các hoạt động trong hệ thống mạng theo thời gian thực, qua đó cảnh báo đến người quản trị để có các biện pháp xử lý kịp thời. Bên cạnh đó việc tích hợp đầy đủ công cụ và hiển thị toàn bộ phân tích tại một trang quản trị sẽ giúp cho người quản trị tiết kiệm thời gian và hiện quả hơn.

Security Onion thực hiện thu thập dữ liệu tại các điểm xác định:

- Xác định các điểm yếu tồn tại trong hệ thống mạng.
- Xác định các nguy cơ có thể ảnh hưởng đến hệ thống.
- Xác định nguồn dữ liệu cần thiết và phân tích nguồn dữ liệu thu thập được.
- Thiết lập trích xuất dữ liệu TAP trên đường truyền để thu thập dữ liệu gói tin.

Sau khi thu thập dữ liệu, Security Onion tiến hành xử lý dữ liệu qua các công cụ được tích hợp sẵn trong gói cài đặt thông qua các quy tắc được xây dựng sẵn. Các dữ liệu được phân tích bao gồm:

Dựa trên mạng:

- Dữ liệu gói tin đầy đủ.
- Dữ liệu phiên truy cập.
- Dữ liệu thống kê băng thông.
- Dữ liệu cảnh báo NIDS dựa vào luật có sẵn và dấu hiệu bất thường.

Dựa trên máy client:

- Dữ liệu nhật ký OS.
- Dữ liệu cảnh báo virus.
- Dữ liệu cảnh báo HIDS.
- Dữ liệu nhật ký Firewall.

Tuy nhiên, ngoài những điểm mạnh của Security Onion còn tồn tại một số nhược điểm như giao diện quản trị tương đối phức tạp và việc tùy biến các quy tắc rất khó khăn, đòi hỏi nhiều thơi gian và kiến thức hơn về hệ thống. Ngoài ra, Security Onion chưa có khả năng back up dữ liệu tự động. Với những điểm nêu ở trên Security Onion chỉ thích hợp với các hệ thống vừa và nhỏ có nguồn kinh phí thấp.

3.4. Kết luận Chương III

Chương này tập trung vào việc cài đặt và triển khai hệ thống Security Onion. Tại chương này giới thiệu chi tiết hơn về yêu cầu cấu trúc, mô hình thiết lập cơ bản cho hệ thống Security Onion. Việc tích hợp các thành phần NIDS, HIDS, giao diện quản trị cũng được làm rõ tại chương này. Các kịch bản xâm nhập hệ thống cũng được chuẩn bi để đánh giá về khả năng hoạt động của hệ thống phát hiện xam nhập Security Onion.

KẾT LUẬN

Luận văn đạt được các sau:

- Mục đích của đề tài hướng nghiên cứu tổng quan nhất về xâm nhập và phát hiện xâm nhập hệ thống thông tin trong mạng LAN. Phân biệt các phương thức tấn công và các giải pháp bảo mật tiêu biểu.

- Bên cạnh đó luận văn cũng tập trung chi tiết vào hệ thống phát hiện xâm nhập Security Onion tích hợp thành phần phát hiện xâm nhập mạng và host. Qua đó cung cấp cho quản trị viên hệ thống một bộ công cụ đầy đủ nhằm theo dõi, phát hiện sớm và cảnh báo các dấu hiệu xâm nhập với chi phí hợp lý.

- Qua các nghiên cứu lý thuyết, luận văn cũng nên các bước cài đặt hệ thống Sercurity Onion trong một mô hình mạng LAN đơn giản. Các kịch bản tấn công cũng được xây dựng trong bài luận để xem xét khả năng hoạt động và đánh giá tính khả thi của hệ thống.

Hướng phát triển của luận văn:

- Xây dựng các tập quy tắc của hệ thống tương thích với thói quen hoạt động của người dùng trong mạng LAN, loại bỏ những cảnh báo không cần thiết tránh lãng phí tài nguyên của hệ thống.

- Tối ưu giao diện hiển thị của Kibana để người quản trị hệ thống nhanh chóng tiếp cận xử lý cảnh báo và dễ dàng thống kê, tạo các báo cáo định kỳ.

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

[1] Hoàng Xuân Dậu, Giáo trình cơ sở an toàn thông tin, Học viện công nghệ BCVT, Nhà xuất bản Thông tin và Truyền thông, 2020.

[2] Luật An ninh mạng Việt Nam năm 2018, ban hành từ ngày 01 tháng 01 năm 2019.

[3] Lê Trung Nghĩa, Nghiên cứu ứng dụng hệ thống phát hiện và ngăn chặn xâm nhập cho hệ thống mạng máy tính dựa trên công nghệ mở, https://ictvietnam.vn/nghien-cuu-ung-dung-he-thong-phat-hien-va-ngan-chan-xam-nhap-cho-he-thong-mang-may-tinh-dua-tren-cong-nghe-mo-8761.htm, truy cập tháng 05 năm 2021.

[4] CSO, Top cybersecurity facts, figures and statistics for 2020, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html, truy cập tháng 8.2020.

[5] IBM QRadar SIEM, https://www.ibm.com/vn-en/products/qradar-siem, truy cập tháng 8.2020.

[6] NortonLifeLock Inc., 10 cyber security facts and statistics for 2018, https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html, truy cập tháng 8.2020.

[7] Snort, https://www.snort.org, truy cập tháng 8.2020.

[8] SolarWinds Security Event Manager, https://www.solarwinds.com, truy cập tháng 8.2020.

[9] Sonicwall Cyber Threat Report, https://www.sonicwall.com/2021-cyber-threat-report/, truy cập tháng 4.2021.

[10] Security Onion, https://securityonion.net, truy cập tháng 8.2020.

[11] OSSEC, https://www.ossec.net, truy cập tháng 8.2020.

[12] Top 10 BEST Intrusion Detection Systems (IDS), https://www.softwaretestinghelp.com/intrusion-detection-systems/, truy cập tháng 5.2021.

[13] 10 Best Network Intrusion Detection Systems Software & NIDS Tools, https://www.comparitech.com/net-admin/nids-tools-software/, truy cập tháng 5.2021