HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN CÔNG HIẾU

NGHIÊN CỨU XÂY DỰNG GIẢI PHÁP PHÁT HIỆN XÂM NHẬP VÀ ỨNG DỤNG CHO HỌC VIỆN THANH THIẾU NIÊN VIỆT NAM

CHUYÊN NGÀNH: KHOA HỌC MÁY TÍNH

MÃ SỐ: 8.48.01.01

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC:

TS. DƯƠNG TRẦN ĐỨC

HÀ NỘI – 2022

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. Dương Trần Đức

Phản biện 1: PGS.TS. PHẠM THANH GIANG

Phản biện 2: PGS.TS. NGUYỄN HÀ NAM

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

Vào lúc: 14 giờ 40 ngày 20 tháng 12 năm 2022

Có thể tìm hiểu luận văn tại:

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

MỞ ĐẦU

Cùng với sự phát triển của mạng Internet, mạng World Wide Web toàn cầu và các dịch vụ trên nền Internet, các dạng tấn công, xâm nhập vào các hệ thống mạng, máy chủ và thiết bị đầu cuối của người dùng cũng phát triển ở mức đáng lo ngại. Các dạng tội phạm trên không gian mạng trở nên rất phổ biến và luôn đứng đầu danh sách truy nã của Cục Điều tra liên bang Mỹ (FBI) trong những năm gần đây [1]. Về mặt địa lý, Việt Nam trong những năm gần đây luôn nằm trong top 10 nước là đích bị tấn công nhiều nhất [1]. Các dạng mã độc và tấn công, khai thác cũng tăng vọt trên các nền tảng di động và IoT. Hãng F-Secure ước tính số lượng tấn công, xâm nhập vào các thiết bị IoT tăng gấp 3 lần trong 6 tháng đầu năm 2019 [2].

Trong số các hệ thống phát hiện tấn công, xâm nhập đang được sử dụng trên thực tế, Snort [2] thuộc nhóm NIDS, là hệ thống mã mở phát hiện tấn công, xâm nhập mã mở được sử dụng rộng rãi nhờ khả năng phát hiện tốt với tập luật dựng sẵn gồm khoảng 3000 luật, hỗ trợ đa nền tảng. Tuy vậy, việc quản lý các sự kiện giám sát và kết quả phát hiện còn tương đối hạn chế cho Snort chỉ hỗ trợ giao diện quản trị cơ bản. Trong khi đó, bộ công cụ quản lý log ELK [5] hỗ trợ xử lý, tìm kiếm và lưu trữ các sự kiện log khá hiệu quả với giao diện thân thiện và dễ sử dụng. Từ đó, luận văn này với đề tài "Nghiên cứu xây dựng giải pháp phát hiện xâm nhập và ứng dụng cho Học viện thanh thiếu niên Việt Nam" có mục tiêu là tập trung nghiên cứu và xây dựng giải pháp phát hiện xâm nhập dựa sử dụng hệ thống phát hiện xâm nhập mạng Snort và bộ công cụ quản lý log ELK có khả năng phát hiện xâm nhập hiệu quả với giao diện quản trị thân thiện.

Luận văn này trước hết tập trung nghiên cứu, khảo sát một số hệ thống phát hiện xâm nhập hiện có trên thị trường. Trên cơ sở kết quả khảo sát sẽ lựa chọn hệ thống phát hiện xâm nhập thích hợp kết hợp với khả năng quản lý log hiệu quả của hệ thống ELK cho triển khai nhằm tăng cường an toàn cho hệ thống mạng của Học viện thanh thiếu niên Việt Nam.

CHƯƠNG 1. TỔNG QUAN VỀ XÂM NHẬP VÀ PHÁT HIỆN XÂM NHẬP

1.1. Tổng quan về 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.

1.1.1. Khái quát về tấn công, xâm nhập

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

1.1.2. Giới thiệu một số dạng tấn công, xâm nhập thường gặp

1.1.2.1 Hình thức tấn công mạng bằng phần mềm độc hại (MalwareAttack)

Tấn công Malware là một trong những hình thức tấn công qua mạng phổ biến nhất hiện nay. Malware bao gồm:

- Spyware (phần mềm gián điệp)
- Ransomware (mã độc tống tiền)
- Virus
- Worm (phần mềm độc hại lây lan với tốc độ nhanh)

1.1.2.2 Hình thức tấn công giả mạo

Phishing Attack là tấn công mà trong đó tin tặc giả mạo thành một cá nhân hoặc tổ chức uy tín để lấy lòng tin của người dùng. Hacker sẽ giả mạo là ví điện tử, ngân hàng, trang giao dịch trực tuyến hoặc các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin cá nhân như: mật khẩu giao dịch, thẻ tín dụng, tài khoản & mật khẩu đăng nhập và các thông tin quan trọng khác. Đây là thủ đoạn tấn công thường dùng và thường là hoạt động mở đầu cho chuỗi các hành động tiếp theo của tin tặc, từ đó, chúng đánh cắp các dữ liệu nhạy cảm như tài khoản ngân hàng, thẻ tín dụng…

1.1.2.3 Hình thức tấn công trung gian

Tấn công trung gian là hình thức tin tặc xen vào giữa phiên giao dịch hay giao tiếp giữa hai đối tượng. Khi đã xâm nhập thành công, chúng có thể theo dõi được mọi hành vi của người dùng. Tệ hơn, chúng có thể đánh cắp được toàn bộ dữ liệu trong phiên giao dịch đó. Tấn công trung gian dễ xảy ra khi nạn nhân truy cập vào một mạng wifi không an toàn

1.1.2.4 Hình thức tấn công từ chối dịch vụ (DoS & DDoS)

Dos – Denial Of Service được dịch ra là từ chối dịch vụ, đây là một hình thức tấn công khá phổ biến khiến cho máy tính mục tiêu không thể xử lý kịp các tác vụ dẫn đến quả tải

Ddos – Distributed Denial Of Service được dịch là từ chối dịch vụ phân tán, hình thức này là một dạng tấn công nỡ lực làm sập một dịch vụ trực tuyến bằng cách làm tràn ngập với traffic từ nhiều nguồn.

Ba loại tấn công cơ bản của Ddos:

- Volume-based: Lưu lượng truy cập cao để làm tràn băng thông
- Protocol: Khai thác các tài nguyên máy chủ
- Application: Tập trung vào các ứng dụng web

1.2 Phát hiện xâm nhập

1.2.1 Khái quát về phát hiện xâm nhập

Là quá trình giám sát các sự kiện xảy ra trong mạng máy tính hoặc một hệ thống máy tính và phân tích để tìm ra các dấu hiệu của sự cố. Các sự cố ở đây có thể là các vi phạm hoặc các mối đe dọa sắp xảy ra vi phạm chính sách bảo mật, chính sách sử dụng được chấp nhận hoặc các phương pháp bảo mật tiêu chuẩn

1.2.2 Phân loại các hệ thống phát hiện xâm nhập

1.2.2.1 Hệ thống phát hiện xâm nhập là gì?

Công nghệ IPS là gì?

Hệ thống phòng chống xâm nhập luôn luôn giám sát bất thường của mạng, đặc biệt là ở các gói riêng lẻ, để tìm kiếm bất kỳ cuộc tấn công nguy hiểm nào có thể xảy ra. Nó thu thập thông tin về các gói tin này và báo cáo cho quản trị viên hệ thống, nhưng nó cũng thực hiện những động thái phòng ngừa của riêng mình. Nếu phát hiện bất thường hoặc loại tấn công khác thì IPS sẽ chặn các gói đó truy cập vào mạng.

IPS có thể ngăn chặn những loại tấn công nào?

Các hệ thống phòng chống xâm nhập có thể bảo vệ tìm kiếm và chống lại nhiều loại tấn công nguy hiểm. Chúng có khả năng phát hiện và chặn các cuộc tấn công tấn công từ chối dịch vụ phân tán (DDoS), từ chối dịch vụ (DoS), virus máy tính, worm, bộ công cụ exploit và những loại phần mềm độc hại khác.

IPS sẽ làm gì nếu nó phát hiện ra một cuộc tấn công?

Một hệ thống ngăn chặn xâm nhập có thể phát hiện nhiều cuộc tấn công khác nhau bằng cách phân tích các gói và tìm kiếm những chữ ký phần mềm độc hại cụ thể, mặc dù nó cũng có thể tận dụng khả năng theo dõi hành vi để tìm kiếm hoạt động bất thường trên mạng, cũng như giám sát bất kỳ giao thức và chính sách bảo mật cấp quản trị nào, cũng như liệu chúng có bị vi phạm hay không.

IDS và IPS có gì khác nhau?

Hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS) đều có thể liên quan đến bảo mật

Hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS) đều có thể liên quan đến bảo mật, nhưng chúng có các mục tiêu và phương tiện hoàn toàn khác nhau.

1.2.2.2 Hệ thống phát hiện xâm nhập bao gồm các loại nào?

Có nhiều loại IDS khác nhau, mỗi loại có một chức năng và nhiệm vụ riêng tuy nhiên hai loại phổ biến nhất là NIDS và HIDS

a. NIDS (Network-Based IDS)

Hệ thống phát hiện xâm nhập mạng (NIDS) được thiết lập tại một điểm được lên kế hoạch trong mạng để kiểm tra lưu lượng truy cập từ tất cả các thiết bị trên mạng. NIDS có thể là các hệ thống dựa trên phần cứng hoặc phần mềm, tùy thuộc vào nhà sản xuất hệ thống, có thể gắn vào các phương tiện mạng khác nhau như Ethernet, FDDI và các phương tiện khác

Ưu điểm của NIDS:

+ Quản lý được cả một network segment (gồm nhiều host)

+ Trong suốt với người sử dụng lẫn kẻ tấn công

+ Bảo trì và cài đặt đơn giản không mất nhiều thời gian, không gây ảnh hưởng gì tới mạng

+ Tránh DOS ảnh hưởng tới một host nào đó

+ Có khả năng xác định lỗi ở tầng Network

+ Độc lập với OS (Operating System)

Nhược điểm của NIDS:

+ Có thể xảy ra trường hợp báo động giả

+ Không phân tích được các dữ liệu đã mã hóa (VD: SSL, SSH, IPSec...)

+ NIDS yêu cầu phải được cập nhật signature mới nhất để được an toàn

+ Phát đi thông báo chậm trễ giữa thời điểm bị tấn công với thời điểm phát báo động. Dẫn đến hệ thống có thể đã bị tổn hại.

+ Không thông báo việc tấn công có thành công hay thất bại

+ Hạn chế lớn nhất là giới hạn băng thông. Bộ dò mạng phải nhận hết các lưu lượng mạng sau đó sắp xếp lại những lưu lượng đó rồi phân tích chúng. Khi tốc độ mạng tăng thì khả năng của đầu dò cũng phải tỉ lệ thuận.

a. HIDS (Hot-Based IDS)

HIDS được cài đặt cục bộ trên một máy tính và do đó linh hoạt hơn nhiều so với NIDS. HIDS có thể được cài đặt trên nhiều loại máy tính cụ thể như máy chủ, máy trạm, máy tính xách tay. HIDS cho phép bạn làm việc linh hoạt trong các phân đoạn mạng mà NIDS không thể. Lưu lượng được gửi đến máy chủ được phân tích và chuyển tiếp đến máy chủ lưu lượng nếu nó không có khả năng độc hại. Trong khi NIDS thậm chí còn tập trung vào mạng lớn chứa các host này. HIDS đặc biệt hướng tới các nền tảng ứng dụng và hướng nhiều đến thị trường Windows trong thế giới máy tính, mặc dù có những sản phẩm hoạt động hiệu quả. Trên nền tảng ứng dụng UNIX và nhiều hệ điều hành khác.

Ưu điểm của HIDS:

+ Có thể xác định người dùng (user) liên quan tới sự kiện (event)

+ NIDS không có khả năng phát hiện các cuộc tấn công diễn ra trên 1 máy còn HIDS thì có thể

+ Có thể phân tích các dữ liệu mã hóa

+ Cung cấp các thông tin về máy chủ (host) trong quá trình tấn công máy chủ này.

Nhược điểm của HIDS:

+ Thông tin của HIDS không đáng tin cậy khi cuộc tấn công vào máy chủ (host) này thành công.

+ Nếu hệ điều hành (OS) bị sập do một cuộc tấn công, đồng thời HIDS cũng sẽ thất bại

+ HIDS phải được thiết lập cấu hình trên từng máy chủ (host) cần giám sát

+ HIDS không thể phát hiện các cuộc dò quét mạng (Nmap, Netcat ...)

+ HIDS cần sử dụng tài nguyên trên máy chủ (host) để hoạt động

+ Khi bị tấn công từ chối dịch vụ DOS, HIDS có thể không hiệu quả

+ Hầu hết HIDS được phát triển trên hệ điều hành Window. Tuy nhiên một số HIDS cũng chạy trên Linux hoặc Unix

1.2.3 Các kỹ thuật phát hiện xâm nhập

1.2.3.1 Statistical anomaly detection:

Liên quan đến việc thu thập dữ liệu liên quan đến hành vi của người dùng hợp pháp trong một khoảng thời gian. Sau đó, các bài kiểm tra thống kê được áp dụng cho hành vi được quan sát để xác định với mức độ tin cậy cao xem hành vi đó có phải là hành vi của người dùng hợp pháp hay không.

- Phát hiện ngưỡng: Cách tiếp cận này liên quan đến việc xác định các ngưỡng, tùy thuộc vào người dùng, cho tần suất xuất hiện của các sự kiện khác nhau.
- Dựa trên hồ sơ: Một hồ sơ của hoạt động của từng người dùng được phát triển và sử dụng để phát hiện những thay đổi trong hành vi của các tài khoản cá nhân.

1.2.3.2 Rule-based detection:

Liên quan đến nỗ lực xác định một tập hợp các quy tắc có thể được sử dụng để quyết định rằng một hành vi nhất định là của một kẻ xâm nhập.

- Phát hiện bất thường: Các quy tắc được phát triển để phát hiện sự sai lệch so với các mẫu sử dụng trước đó.
- Thâm nhập nhận dạng: Một phương pháp tiếp cận hệ thống chuyên gia tìm kiếm hành vi đáng ngờ.

Tóm lại, các phương pháp thống kê cố gắng xác định hành vi bình thường hoặc được mong đợi, trong khi các phương pháp tiếp cận dựa trên quy tắc cố gắng xác định hành vi phù hợp.

Về mặt các loại kẻ tấn công được liệt kê trước đó, phát hiện bất thường thống kê có hiệu quả chống lại những kẻ giả mạo, những kẻ không có khả năng bắt chước các mô hình hành vi của các tài khoản mà họ thích hợp. Mặt khác, những kỹ thuật như vậy có thể không đối phó được với những kẻ thất bại. Đối với các cuộc tấn công như vậy, các phương pháp tiếp cận dựa trên quy tắc có thể nhận ra các sự kiện và trình tự, trong ngữ cảnh, cho thấy sự thâm nhập. Trong thực tế, một hệ thống có thể thể hiện sự kết hợp của cả hai cách tiếp cận để có hiệu quả chống lại một loạt các cuộc tấn công.

CHƯƠNG 2. CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP VÀ QUẢN LÝ LOG

2.1 CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP

Snort, Suricata, Zeek và IBM Qradar là các hệ thống trong những hệ thống phát hiện xâm nhập phổ biến hiện nay sở hữu nhiều tính năng nổi bật cũng như được sử dụng rộng rãi bởi các cơ quan, tổ chức.

2.1.1 Snort

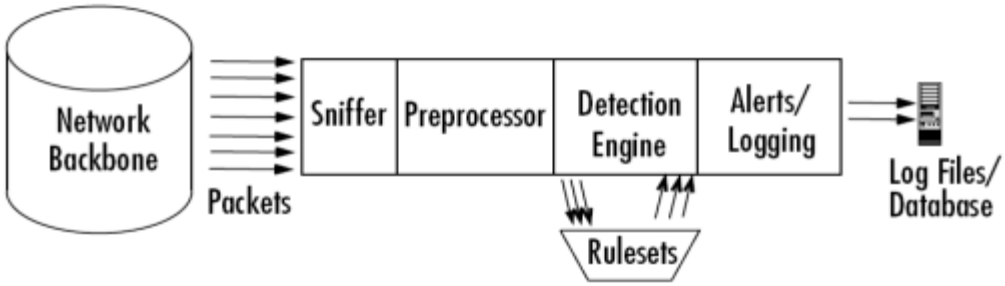
Snort hoạt động ở 3 chế độ chính là:

- Chế độ Sniffer, cho phép Snort đọc các gói tin trên mạng và hiển thị chúng lên màn hình.

- Chế độ Packet Logger, sẽ thực hiện ghi logs các gói tin thu thập được vào ổ đĩa dưới dạng tệp tin văn bản hoặc tệp tin nhị phân.

- Với chế độ Network Intrusion Detection System (NIDS), Snort sẽ thực hiện giám sát lưu lượng mạng, phân tích và đối chiếu chúng với một tập luật được định nghĩa bởi người dùng để phát hiện các xâm nhập. Đây cũng là chế độ phức tạp và nhiều tùy chỉnh nhất của Snort.

Về kiến trúc của Snort, bao gồm 5 phần chính như sau



2.1.2 Suricata

Suricata là một công cụ Giám sát an ninh mạng NSM (Network Security Mornitoring), phát hiện và ngăn chặn IDS/IPS (Intrusion Detection System/Intrusion Prevention System) mạng hiệu suất cao [4]. Suricata là mã nguồn mở được phát triển bởi OISF (Open Information Security Foundation) và do cộng đồng điều hành. Nó hoạt động rất tốt với khả năng kiểm tra gói sâu và đối sánh mẫu, điều này khiến Suricata trở nên vô cùng hữu ích trong việc phát hiện các mối đe dọa và tấn công.

2.1.3 Zeek

Zeek là một công cụ phân tích lưu lượng mạng mã nguồn mở thụ động. Nhiều nhà khai thác sử dụng Zeek như một trình giám sát an ninh mạng (NSM) để hỗ trợ các cuộc điều tra về hoạt động đáng ngờ hoặc độc hại. Zeek cũng hỗ trợ một loạt các nhiệm vụ phân tích lưu lượng ngoài phạm vi bảo mật, bao gồm đo lường hiệu suất và khắc phục sự cố.

2.1.4 IBM Qradar

IBM Qradar là một hệ thống tích hợp các chức năng thu thập, xử lý, tổng hợp và lưu trữ dữ liệu mạng trong thời gian thực. Qradar sử dụng dữ liệu đó để quản lý an ninh mạng bằng cách cung cấp thông tin và giám sát theo thời gian thực, cảnh báo và hành vi vi phạm cũng như phản ứng với các mối đe dọa mạng.

Thành phần và chức năng.

Hoạt động của nền tảng thông minh bảo mật Qradar bao gồm ba lớp và áp dụng cho bất kỳ cấu trúc triển khai Qradar nào, bất kể quy mô và độ phức tạp của nó. Sơ đồ sau đây cho thấy các lớp tạo nên kiến trúc Qradar .

- Event collector component
- Event processor component
- Magistrate

2.1.5 So sánh các hệ thống phát hiện xâm nhập

Tiêu chí	SNORT	SURICATA	ZEEK	IBM QRADAR
Luồng xử lý	Đơn luồng	Đa luồng	Đơn luồng	Đa luồng
Sử dụng tài nguyên hệ thống	Trung bình	Nhiều	Ít	Nhiều
Tỷ lệ bỏ qua gói tin khi lưu lượng ít	Cao	Thấp	Trung bình	Thấp
Kỹ thuật phát hiện xâm nhập	Signature-based IDS	Signature-based IDS	Signature-based IDS và Anomaly-based IDS	Signature-based IDS

Tập luật	Sử dụng các luật từ VRT, Emerging Threat, cũng như là các tập luật được viết bởi cộng đồng	Sử dụng các luật từ VRT, Emerging Threat. Ngoài ra còn hỗ trợ các luật được viết bằng Lua script.	Sử dụng các luật được viết bằng chính Zeek script	Công cụ quy tắc tùy chỉnh (CRE)
Kết quả đầu ra	Có thể ghi kết quả đầu ra dưới dạng Syslog, tcpdump, csv hoặc unified2.	Cho phép ghi kết quả đầu ra dưới dạng Eve json và syslog. Ngoài ra còn hỗ trợ dùng Lua script để lấy kết quả đầu ra	Mặc định ghi kết quả đầu ra dưới dạng ASCII. Có thể tùy chỉnh để ghi dưới định dạng JSON hoặc ghi vào SQLite	Chuyển tiếp dữ liệu tới các mục tiêu ngoại vi, hệ thống Syslog bên ngoài, hệ thống JSON và các SIEM khác.
Hệ điều hành hỗ trợ	Linux, FreeBSD, OpenBSD, MacOS, Windows	Linux, FreeBSD, MacOS, Windows	Linux, FreeBSD, MacOS	Linux, Windows

2.2 HỆ THỐNG QUẢN LÝ LOG ELK

Hệ thống quản lý log ELK hay còn gọi là ELK Stack là một bộ sưu tập của ba sản phẩm mã nguồn mở - Elasticsearch, Logstash, và Kibana [15]. ELK Stack cung cấp ghi nhật ký tập trung để xác định các sự cố với máy chủ hoặc ứng dụng. Nó cho phép bạn tìm kiếm tất cả các bản ghi ở một nơi duy nhất. Nó cũng giúp tìm ra sự cố trong nhiều máy chủ bằng cách kết nối các bản ghi trong một khung thời gian cụ thể.

- E là viết tắt của ElasticSearch: dùng để lưu trữ nhật ký.

- L là viết tắt của LogStash: được sử dụng cho cả vận chuyển cũng như xử lý và lưu trữ nhật ký.

- K là viết tắt của Kibana: là một công cụ trực quan hóa (một giao diện web) được lưu trữ thông qua Nginx hoặc Apache

2.2.1 Elasticsearch

Elasticsearch là một cơ sở dữ liệu NoSQL. Nó dựa trên công cụ tìm kiếm Lucene và nó được xây dựng với RESTful APIS. Nó cung cấp triển khai đơn giản, độ tin cậy tối đa và quản lý dễ dàng. Nó cũng cung cấp các truy vấn nâng cao để thực hiện phân tích chi tiết và lưu trữ tất cả dữ liệu một cách tập trung. Nó rất hữu ích để thực hiện tìm kiếm nhanh các tài liệu.

Elasticsearch cũng cho phép bạn lưu trữ, tìm kiếm và phân tích khối lượng lớn dữ liệu. Nó chủ yếu được sử dụng làm công cụ cơ bản để cung cấp năng lượng cho các ứng dụng đã hoàn thành các yêu cầu tìm kiếm. Nó đã được áp dụng trong các nền tảng công cụ tìm kiếm cho các ứng dụng web và di động hiện đại. Ngoài tính năng tìm kiếm nhanh, công cụ này còn cung cấp các phân tích phức tạp và nhiều tính năng nâng cao.

2.2.2 Logstash

Logstash là công cụ đường ống thu thập dữ liệu. Nó thu thập dữ liệu đầu vào và cấp dữ liệu vào Elasticsearch. Nó thu thập tất cả các loại dữ liệu từ các nguồn khác nhau và làm cho nó có sẵn để sử dụng thêm.

Các tính năng của Logstash bao gồm: các sự kiện được chuyển qua từng giai đoạn bằng cách sử dụng hàng đợi nội bộ, cho phép các đầu vào khác nhau cho nhật ký, lọc/phân tích cú pháp các nhật ký.

Lợi thế của Logstash: cung cấp tập trung dữ liệu, phân tích nhiều loại dữ liệu và sự kiện có cấu trúc/phi cấu trúc, cung cấp các plugin để kết nối với nhiều loại nguồn và nền tảng đầu vào khác nhau.

2.2.3 Kibana

Kibana là một công cụ trực quan hóa dữ liệu hoàn thành ngăn xếp ELK. Công cụ này được sử dụng để trực quan hóa các tài liệu Elasticsearch và giúp các nhà phát triển có cái nhìn sâu sắc về nó. Bảng điều khiển Kibana cung cấp các sơ đồ tương tác, dữ liệu không gian địa lý và đồ thị khác nhau để hình dung các quy tắc phức tạp. Nó có thể được sử dụng để tìm kiếm, xem và tương tác với dữ liệu được lưu trữ trong các thư mục Elasticsearch. Kibana giúp bạn thực hiện phân tích dữ liệu nâng cao và trực quan hóa dữ liệu của bạn trong nhiều bảng, biểu đồ và bản đồ.

CHƯƠNG 3.
XÂY DỰNG VÀ THỬ NGHIỆM MÔ HÌNH GIẢI PHÁP PHÁT HIỆN XÂM NHẬP DỰA TRÊN SNORT VÀ ELK CHO HỆ THỐNG MẠNG HỌC VIỆN THANH THIẾU NIÊN VIỆT NAM

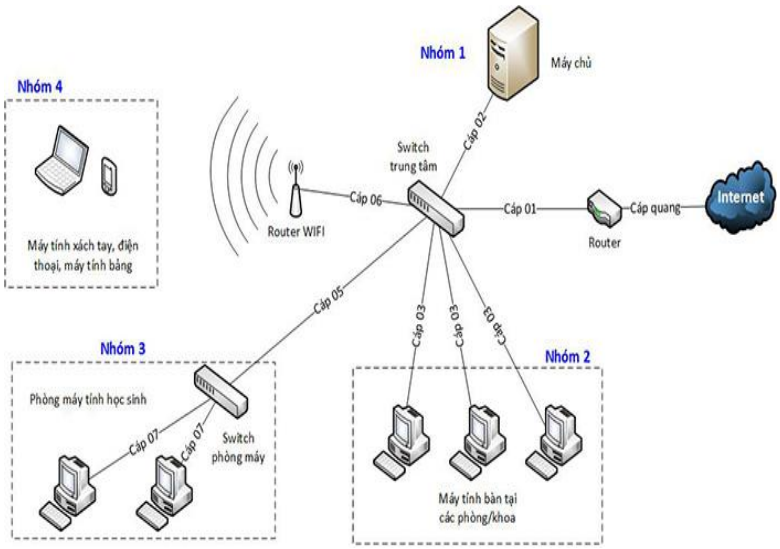
3.1. Khảo sát và triển khai mô hình

3.1.1 Khảo sát hệ thống mạng tại Học viện Thanh thiếu niên Việt Nam

Hình 3.1 Phối cảnh tổng thể Học viện Thanh thiếu niên Việt Nam

Trường Học viện Thanh thiếu niên Việt Nam được xây dựng trên diện tích 13 ha bao gồm 163 phòng học và giảng đường đạt tiêu chuẩn, 17 phòng thực hành, thí nghiệm; ngoài ra còn có nhà tập Đa năng; Phòng làm việc của Giáo sư, phó Giáo sư, giảng viên của cơ sở đào tạo là 50, Trung tâm thư viện hiện đại với diện tích trên 640m2 đã đưa vào sử dụng; sân bãi, 1 tòa nhà hiệu bộ 11 tầng đang được xây dựng và nhiều trang thiết bị khác đáp ứng đủ nhu cầu dạy học

3.1.1.1 Sơ đồ mạng



Hình 3.2 Mô hình mạng máy tính trường Học viện Thanh thiếu niên Việt Nam

Cụ thể hệ thống mạng được chia làm các vùng sau:

- Nhóm 1:Hệ thống máy chủ
- Nhóm 2:Máy tính tại các phòng ban, khoa
- Nhóm 3:Hệ thống máy tính phòn thực hành
- Nhóm 4:Máy tính xách tay, điện thoại, máy tính bảng

3.1.1.2 Những tồn tại của hệ thống mạng tại trường.

Hiện nay, trường chưa được cài hệ thống tường lửa để bảo vệ toàn thể máy tình các phòng ban, các khu vực mạng tránh khỏi các hiểm họa, nguy cơ về an toàn thông tin, các rủi ro có thể ảnh hưởng tới hệ thống mạng :

- Các cuộc tấn công vào khu vực DMZ khi mà các vùng đó chạy dịch vụ: DNS, web, mail.
- Các tấn công tới người dùng (Social engineering) trong mạng.
- Tấn công vào mạng LAN của trường
- Tấn công nghe trộm trên đường truyền
- Tấn công từ chối dịch vụ vào các hệ thống mạng văn phòng của phòng, ban.
- Tấn công bằng mã độc vào hệ thống mạng thông qua các phương tiện khác hoặc người dung. Mạng chưa có hệ thống cân bằng tải, hệ thống dự phòng, vv.. do vậy tính sẵn sàng của hệ thống còn nhiều điểm hạn chế.
- Xâm nhập vật lý tới các thiết bị cụ thể của hệ thống

3.1.2 Mô hình triển khai

Hệ thống thử nghiệm được triển khai cài đặt gồm 2 máy như sau:

- Máy Kali Linux sử dụng các công cụ để thực hiện các kịch bản tấn công mạng đến máy mục tiêu là máy Ubuntu chạy SNORT và ELK
- Máy Ubuntu cài đặt và cấu hình hệ thống phát hiện xâm nhập SNORT và ELK để đưa ra cảnh báo.

- **Môi trường giả lập:** VMware Workstation Pro 12
- **Thiết lập cấu hình:**

✓ Client: Windows 10 – **Vmnet 11: 192.168.11.12**

✓ Attacker: Kali Linux 2016.2 – **Vmnet 11: 192.168.11.10**

✓ Snort IDS/IPS: CentOS 6.8 – **Vmnet 11: 192.168.11.11/24**

Vmnet 12: 192.168.10.12/24

✓ WEB Server: CentOS 6.8 – **Vmnet 12: 192.168.10.13**

3.2 Cài đặt và cấu hình hệ thống phát hiện xâm nhập

3.2.1. Cài đặt snort IDS

✓ **Cài đặt Package yêu cầu:**

```
# yum install -y gcc flex bison zlib* libxml2 libpcap* pcre* tcpdump git libtool curl daq
# yum groupinstall - y "Development Tools"
```

✓ **Tải và cài đặt các file cài đặt riêng sau:**

libdnet-1.12.tgz

libdnet-1.12-6.el6.x86_64.rpm

libdnet-devel-1.12-6.el6.x86_64.rpm

✓ **Tải file snort mới nhất tại https://snort.org**

daq-2.0.6.tar

snort-2.9.8.3.tar

✓ **Bắt đầu cài đặt snort**

```
# cd /usr/local/src
# tar -zxvf /root/ips/daq-2.0.6.tar.gz
# tar -zxvf /root/ips/snort-2.9.8.3.tar.gz
```

cd daq-2.0.6

./configure

make && make install

cd /usr/local/src/snort-2.9.8.3

./configure

make && make install

cd /etc

mkdir snort

cd snort

cp /usr/local/src/snort-2.9.8.3/etc/* .

tar -zvxf /root/ips/snortrules-snapshot-2983.tar.gz

touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules

- ✓ **Cấu hình snort:**

vim /etc/snort/snort.conf

output alert_unified2: *filename snort.alert, limit 128, nostamp*

output log_unified2: *filename snort.log, limit 128, nostamp*

ipvar HOME_NET any > *ipvar HOME_NET 192.168.10.0/24*

ipvar EXTERNAL_NET any > *ipvar EXTERNAL_NET !$HOME_NET*

var RULE_PATH ../rules > *var RULE_PATH /etc/snort/rules*

var SO_RULE_PATH ../so_rules > *var SO_RULE_PATH /etc/snort/so_rules*

var PREPROC_RULE_PATH ../preproc_rules > *var PREPROC_RULE_PATH /etc/snort/preproc_rules*

var WHITE_LIST_PATH ../rules > *var WHITE_LIST_PATH /etc/snort/rules*

var BLACK_LIST_PATH ../rules > *var BLACK_LIST_PATH /etc/snort/rules*

“Esc : wq!” lưu cấu hình vào file.

cd /usr/local/src

chown -R snort:snort daq-2.0.6

chown -R 777 daq-2.0.6

chown -R snort:snort snort-2.9.8.3

chown -R 777 snort-2.9.8.3

chown -R snort:snort snort_dynamicsrc

chown -R 777 snort_dynamicsrc

3.2.2. Cài đặt snort IPS: snort inline mode

Mở cấu hình snort inline mode trong snort.conf:

vim /etc/snort/snort.conf

"**##** Under Step **#2**:" Thêm dòng sau:

config policy_mode:inline

Cấu hình giá trị biến DAQ để chạy **AFPacket** trong inline (IPS) mode:

"## Configure DAQ variables for AFPacket"

config daq: *afpacket*

config daq_mode: *inline*

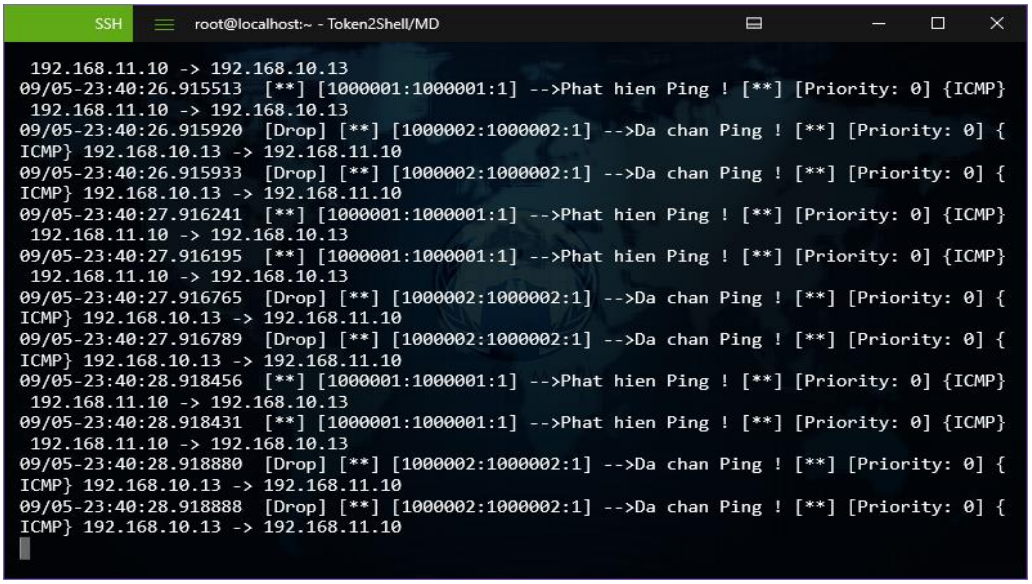
config daq_dir: */usr/local/lib/daq*

config daq_var: *buffer_size_mb=128*

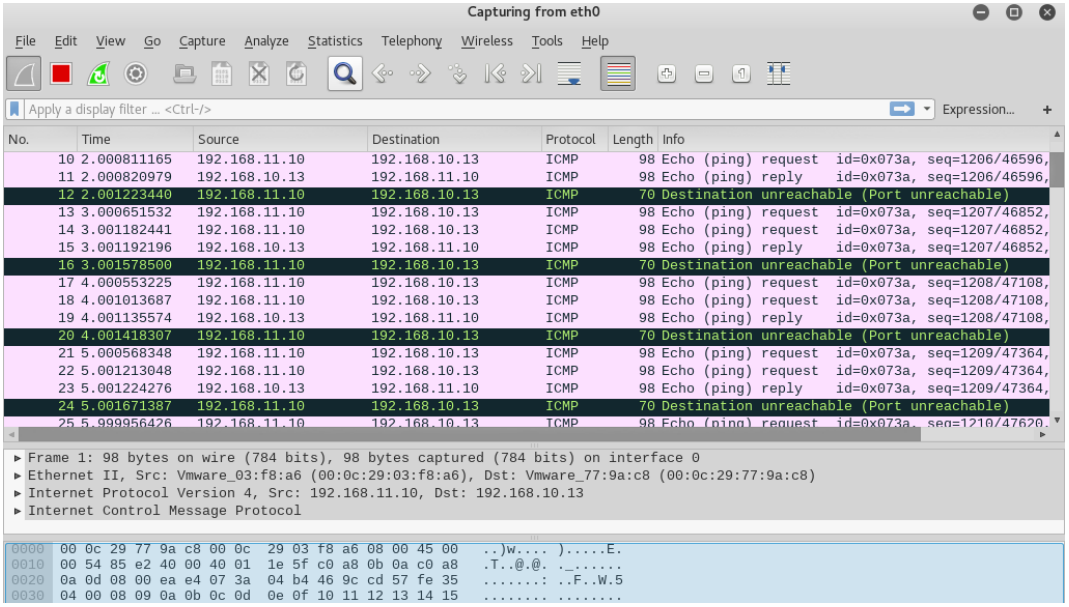
Lưu cấu hình. Thêm rule chặn ping và kiểm tra:

drop icmp any any -> any any (itype:0;msg:"-->Da chan Ping !";gid:1000002;sid:1000002;rev:1;)

snort -i eth1:eth2 -A console -c /etc/snort/snort.conf -l /var/log/snort/ -Q



Hình 3.5 Snort IPS đã phát hiện và chặn (DROP) các gói PING icmp từ Attacker



Hình 3.6 Các gói tin có giao thức ICMP đã bị chặn (drop) trên máy của Attacker

3.3. Cài đặt BASE quản lý phân tích Snort Log trên web

- BASE (Basic Analysis and Security Engine) cung cấp một trang web front-end để truy vấn và phân tích cảnh báo từ Snort. Các cảnh báo sẽ gửi đến một cơ sở dữ liệu MySQL, tính năng này được cung cấp bởi barnyard2 .

- Barnyard2 là một hệ thống đầu ra cho Snort, nó đọc các bản ghi nhị phân từ snort sử dụng định dạng unified2 và sau đó nó sẽ gửi lại các thông tin của bản ghi này tới cơ sở dữ liệu của user thiết lập trong mysql.

→Yêu cầu: đã cài sẵn PHP, Mysql, httpd

✓ **Cài đặt các gói yêu cầu cho BASE:**

```
# pear channel-update pear.php.net
# pear install Mail Mail_mime
# pear install Numbers_Roman
# pear install Image_Color-1.0.4
# pear install Image_Canvas-0.3.5
# pear install Image_Graph-0.8.0
```

✓ **Khởi động lại snort:**

```
# /etc/init.d/snortd restart
```

- ✓ **Cài đặt Adodb:**

cd /root/ips

wget http://jaist.dl.sourceforge.net/project/adodb/adodb-php5-only/adodb-520-for-php5/adodb-5.20.6.zip

unzip adodb-5.20.6.zip

mv adodb5 /var/www/adodb

- ✓ **Cài đặt BASE:**

cd /root/ips

wget http://nchc.dl.sourceforge.net/project/secureideas/BASE/base-1.4.5/base-1.4.5.tar.gz

mkdir /var/www/html/base

tar -xzvf /root/ips/base-1.4.5.tar.gz

cp -r base-1.4.5/* /var/www/html/base

chown -R snort:snort /var/www/html/base

cd /var/www/html/base

cp base_conf.php.dist base_conf.php

chmod 755 /var/www/html/base/base_conf.php

vim /var/www/html/base/base_conf.php

$BASE_urlpath = '/base';

$DBlib_path = '/var/adodb';

$alert_dbname = 'snort';

$alert_host = 'localhost';

$alert_port = '3306';

$alert_user = 'snort';

$alert_password = '123456';

 # chmod 777 /var/www/html/base

- ✓ **Cấu hình Apache:**

vim /etc/httpd/conf/httpd.conf

Alias /base /var/www/html/base/

<Directory "/var/www/html/base/">

AllowOverride None

Order allow,deny

Allow from all

</directory>

Alias /adodb/ "/var/adodb/"

<Directory "/var/adodb">

AllowOverride None

Order allow,deny

Allow from all

</Directory>

vim /etc/httpd/conf.d/base.conf

Alias /base /var/www/html/base/

<directory "/var/www/base/">

AllowOverride None

Order allow,deny

Allow from all

AuthName "Snort IDS"

AuthType Basic

AuthUserFile /etc/snort/base.passwd

Require valid-user

</directory>

- ✓ **Tạo file khẩu để truy cập web cho database:**

htpasswd -c /etc/snort/base.passwd snortadmin

service httpd restart

chcon -R -t httpd_sys_content_t /var/www/html/base/

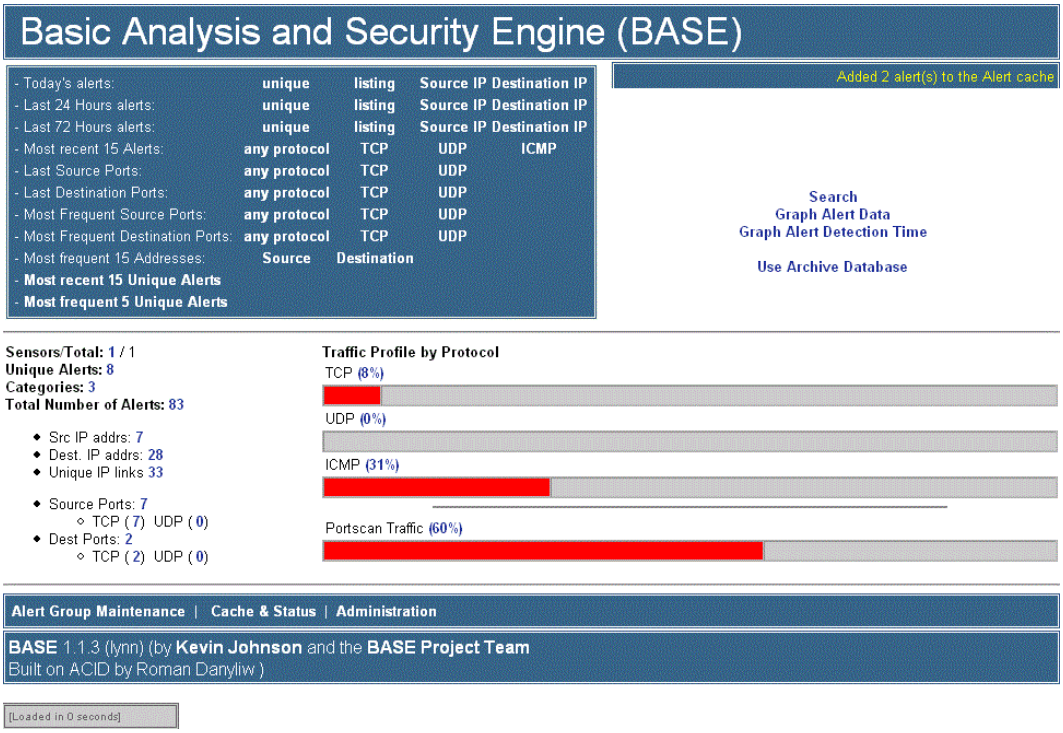
chcon -R -h -t httpd_sys_content_t /var/www/adodb

vim /var/www/html/base/base_main.php

date_default_timezone_set('Asia/Ho_Chi_Minh');

→Truy cập giao diện web để cài đặt base và quản lý:

http://192.168.0.100/base/base_db_setup.php



Hình 3.7 Giao diện chính của BASE trên web

3.4 Cài đặt ELK Stack

Server cài đặt ở đây thực hiện trên CentOS 8, trước tiên cần đảm bảo cài đặt Java (openjdk)

yum update -y

yum install java-1.8.0-openjdk-devel -y

Trước khi tiến hành cài đặt các thành phần của Elastic Stack, ta cần tải xuống và cài đặt khóa công khai của Elastic

sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

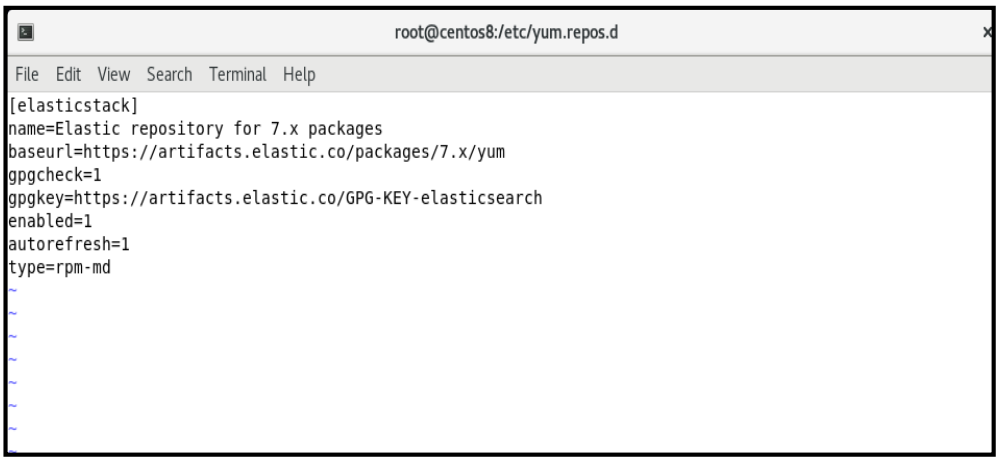
Thao tác này sẽ thêm khóa ký công khai Elasticsearch vào hệ thống của bạn. Khóa này sẽ xác thực phần mềm Elasticsearch khi bạn tải xuống.

Thêm kho lưu trữ Elasticsearch bằng cách tạo tệp cấu hình kho lưu trữ : **elasticsearch.repo** trong thư mục **/etc/yum.rpos.d/**

cd /etc/yum.repos.d/

sudo vim elasticsearch.repo #

nhập nội dung sau



Hình 3.8 Cấu hình kho lưu trữ RPM Elasticsearch

Sau đó cập nhật các gói trong kho lưu trữ bằng lệnh

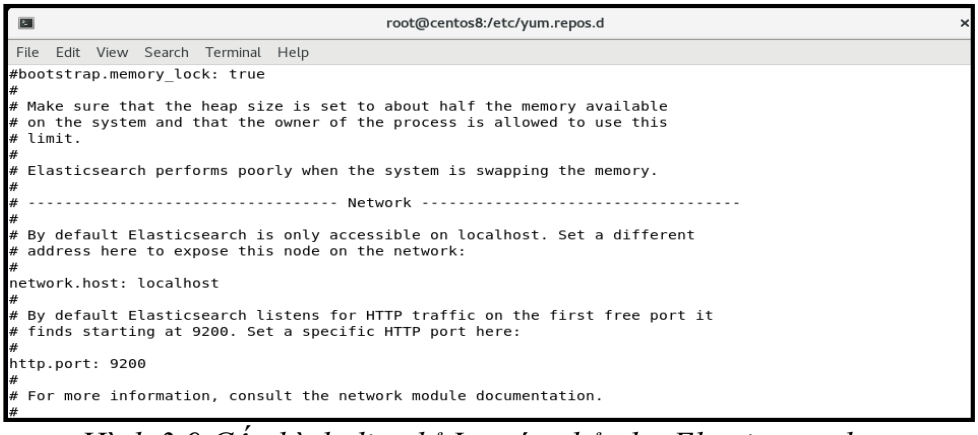
dnf update

Tiếp theo cài đặt và thiết lập Elasticsearch

sudo dnf install elasticsearch

Sau khi quá trình cài đặt kết thúc, mở và chỉnh sửa địa chỉ ip máy chủ trong file **/etc/elasticsearch/elasticsearch.yml**

sudo vim /etc/elasticsearch/elasticsearch.yml



Hình 3.9 Cấu hình địa chỉ Ip máy chủ cho Elasticsearch

Khởi động lại hệ thống, sau đó khởi động dịch vụ **elasticsearch** đồng thời kích hoạt tính năng dịch vụ **elasticsearch** khi hệ thống khởi động

sudo systemctl start elasticsearch sudo systemctl enable elasticsearch

Tiếp theo, ta cài đặt và thiết lập Kibana

sudo dnf install kibana

Thiết lập cấu hình cho Kibana trong file kibana.yml tại thư mục

/etc/kibana/

Khởi động và kích hoạt Kibana *sudo*

systemctl start kibana sudo

systemctl enable kibana

3.5. Cài đặt Filebeat

Cài đặt modul Filebeat

yum install filebeat

filebeat modules enable system

filebeat setup

service filebeat start

Theo mặc định, Filebeat ghi trực tiếp file vào Elasticsearch. Để tùy chỉnh Filebeat, hãy chỉnh sửa file cấu hình **/etc/filebeat/filebeat.yml**.

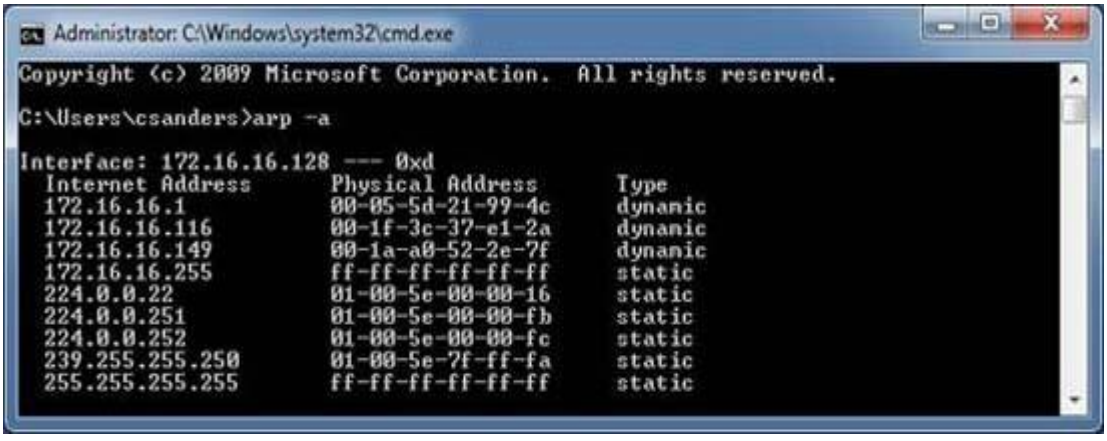
Sau khi cài đặt xong Filebeat khởi chạy modul Suricata filebeat modules enable suricata

3.6. Một số phương thức tấn công và cách phòng chống

3.6.1. ARP Spoofing Attack

Cách phòng chống: Mã hóa ARP cache

Một cách có thể bảo vệ chống lại vấn đề không an toàn vốn có trong các ARP request và ARP reply là thực hiện một quá trình kém động hơn. Đây là một tùy chọn vì các máy tính Windows cho phép bạn có thể bổ sung các entry tĩnh vào ARP cache. Bạn có thể xem ARP cache của máy tính Windows bằng cách mở Commad Prompt và gõ lệnh arp –a.



Hình 3.10 Xem ARP Cache

Có thể thêm các entry vào danh sách này bằng cách sử dụng lệnh:

arp –s <IP ADDRESS> <MAC ADDRESS>.

Trong các trường hợp, nơi cấu hình mạng của bạn không mấy khi thay đổi, bạn hoàn toàn có thể tạo một danh sách các entry ARP tĩnh và sử dụng chúng cho các client thông qua một kịch bản tự động. Điều này sẽ bảo đảm được các thiết bị sẽ luôn dựa vào ARP cache nội bộ của chúng thay vì các ARP request và ARP reply.

3.6.2. SYN Flood Attack

Cách phòng chống: Sử dụng Iptables hoặc Snort IPS

Sử dụng Iptables:

```
# iptables  -A INPUT –p tcp --syn –m limit --limit 1/s --limit  -burst 3 -j RETURN
```

Tất cả các kết nối đến hệ thống chỉ được phép theo các thông số giới hạn sau:

- **--limit 1/s**: Tốc độ truyền gói tin trung bình tối đa 1/s (giây)
- **--limit-burst 3**: Số lương gói tin khởi tạo tối đa được phép là 3

Sử dụng Snort IPS thêm rule sau:

```
dropt tcp any any -> $HOME_NET any (msg:"-->Da chan SYN FIN Attack ! "; flags:
S;gid: 2000001;sid:2000001;)
```

3.6.3. Zero Day Attack

Cách phòng chống:

+ Cập nhật bản vá lỗi.

+ Lọc dữ liệu từ cổng TCP 445 bằng tường lửa (iptables).

+ Khóa cổng SMB trong registry.

3.6.4. DOS - Ping Of Death Attack

Cách phòng chống:

Sử dụng các tính năng cho phép đặt rate limit trên router/firewall để hạn chế số lượng packet vào hệ thống.

Dùng tính năng lọc dữ liệu của router/firewall để loại bỏ các packet không mong muốn, giảm lượng lưu thông trên mạng và tải của máy chủ.

Sử dụng Snort IPS và thêm rule:

```
drop icmp any any -> $HOME_NET any (msg:"-->Da chan Ping Of Dead !";
dsize:>20000; gid:1000002; sid:1000002;rev:1;)
```

KẾT LUẬN

Các kết quả đạt được:

Luận văn này tập trung nghiên cứu về thu thập, xử lý, phân tích log truy cập, phục vụ phát hiện các hành vi bất thường và nguy cơ mất an toàn thông tin trong các hệ thống mạng. Các nội dung đã thực hiện trong luận văn bao gồm:

- Trình tổng quan về tấn công, xâm nhập mạng, các dạng tấn công xâm nhập thường gặp; đồng thời cũng đã khái quát về phát hiện xâm nhập cũng như các kỹ thuật phát hiện xâm nhập qua đó ta có cái nhìn rõ hơn về tấn công, xâm nhập.

- Mô tả một số nền tảng về công cụ xử lý và phân tích log truy nhập, từ đó rút ra so sánh, đánh giá để tìm ra mô hình triển khai phù hợp.

- Trình bày kiến trúc, hoạt động tính năng của các hệ thống xâm nhập mạng phổ biến hiện nay là Snort, Suricata và Zeek. Từ đó, đưa ra so sánh về ưu, nhược điểm của các hệ thống này. Giới thiệu các hệ thống phát hiện xâm nhập tích hợp IBM QRadar và bộ công cụ quản lý log Elastic Stack.

- Cài đặt hệ thống phát hiện tấn công, xâm nhập mạng với nền tảng mã nguồn mở như Snort và ELK. Thử nghiệm các kịch bản tấn công cụ thể và đưa ra kết quả cảnh báo khi bị tấn công.