|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  Logo HvKTMM |
| ĐỀ TÀI PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH  **Tìm hiểu về điều tra mạng :**  **Chương 5. Theo dõi kẻ xâm nhập qua mạng** |
| *Sinh viên thực hiện:*   |  |  | | --- | --- | | Hoàng Quốc Anh | AT12B | | Thân Hữu Tuấn | AT12B | | Nguyễn Khắc Toàn | AT12B |   **Hà Nội - 2019** |

# MỤC LỤC

[MỤC LỤC i](#_Toc25793469)

[DANH MỤC TỪ VIẾT TẮT iii](#_Toc25793470)

[DANH MỤC BẢNG BIỂU HÌNH VẼ iv](#_Toc25793471)

[MỞ ĐẦU v](#_Toc25793472)

[CHƯƠNG 1. TÌM HIỂU TỔNG QUAN VỀ ĐIỀU TRA MẠNG 1](#_Toc25793473)

[1.1. Giới thiệu về điều tra số 1](#_Toc25793474)

[1.1.1. Khái niệm 1](#_Toc25793475)

[1.1.2. Mục đích và ứng dụng 1](#_Toc25793476)

[1.2. Các loại hình điều tra phổ biến 2](#_Toc25793477)

[1.2.1. Điều tra máy tính 2](#_Toc25793478)

[1.2.2. Điều tra mạng 3](#_Toc25793479)

[1.2.3. Điều tra thiết bị di động 3](#_Toc25793480)

[CHƯƠNG 2. THEO DÕI KẺ XÂM NHẬP TRÊN MẠNG 5](#_Toc25793481)

[2.1. Tìm hiểu về hệ thống phát hiện xâm nhập 5](#_Toc25793482)

[2.1.1.Tổng quan về hệ thống phát hiện xâm nhập 5](#_Toc25793483)

[2.1.2. Tìm hiểu về hệ thống ngăn chặn xâm nhập mạng 7](#_Toc25793484)

[2.2. Phương thức phát hiện 8](#_Toc25793485)

[2.2.1. So trùng mẫu (Pattern matching) 8](#_Toc25793486)

[2.2.2. Dấu hiệu bất thường (anomaly detection) 9](#_Toc25793487)

[2.3. Phân biệt giữa NIDS và NIPS 10](#_Toc25793488)

[2.4. Sử dụng Snort để phát hiện, ngăn chặn xâm nhập mạng 13](#_Toc25793489)

[2.4.1. Giới thiệu 13](#_Toc25793490)

[2.4.2. Sử dụng snort để phát hiện, ngăn chặn xâm nhập mạng 14](#_Toc25793491)

[CHƯƠNG 3. THỰC NGHIỆM PHÁP HIỆN XÂM NHẬP MẠNG VỚI SNORT 25](#_Toc25793492)

[3.1. Mô hình thử nghiệm 25](#_Toc25793493)

[3.2. Cài đặt snort 25](#_Toc25793494)

[3.2.1. Chuẩn bị 25](#_Toc25793495)

[3.2.2. Cài đặt Snort 26](#_Toc25793496)

[3.2.3. Cấu hình Snort chạy NIDS mode 26](#_Toc25793497)

[3.3. Thiết lập luật cơ bản 28](#_Toc25793498)

[KẾT LUẬN 30](#_Toc25793499)

[DANH MỤC TÀI LIỆU THAM KHẢO 31](#_Toc25793500)

# DANH MỤC TỪ VIẾT TẮT

|  |  |
| --- | --- |
| **Từ viết tắt** | **Ý nghĩa** |
| NIDS | Network Intrusion Detection System |
| NIPS | Network-based Intrusion Prevention System |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| RAM | Random Access Memory |
| GPS | Global Positioning System |
| UTM | Unified Threat Management |

# DANH MỤC BẢNG BIỂU HÌNH VẼ

[*Hình 2. 1. Mô hình NIDS 10*](#_Toc25798326)

[*Hình 2. 2. Mô hình NIPS 11*](#_Toc25798327)

[*Hình 2. 3. Thiết lập snort trên windows 1 14*](#_Toc25798328)

[*Hình 2. 4. Thiết lập snort trên windows 2 14*](#_Toc25798329)

[*Hình 2. 5. Thiết lập snort trên windows 3 15*](#_Toc25798330)

[*Hình 2. 6. Thiết lập snort trên windows 4 16*](#_Toc25798331)

[*Hình 2. 7. Thiết lập snort trên windows 5 16*](#_Toc25798332)

[*Hình 2. 8. Thiết lập snort trên windows 6 17*](#_Toc25798333)

[*Hình 2. 9. Thiết lập snort trên windows 7 17*](#_Toc25798334)

[*Hình 2. 10. Thiết lập snort trên windows 8 18*](#_Toc25798335)

[*Hình 2. 11. Kết quả câu lệnh 1 19*](#_Toc25798336)

[*Hình 2. 12. Kết quả câu lệnh 2 20*](#_Toc25798337)

[*Hình 2. 13. Kết quả câu lệnh 3 21*](#_Toc25798338)

[*Hình 3. 1. Mô hình thử nghiệm 25*](#_Toc25798339)

[*Hình 3. 2. Kết quả thực nghiệm 29*](#_Toc25798340)

[*Bảng 2. 1. Bảng liệt kê các trạng thái cảnh báo của NIDS 6*](#_Toc25798435)

# MỞ ĐẦU

Sự phát triển mạnh mẽ của Công nghệ thông tin nói chung và mạng Internet nói riêng đã tạo điều kiện thuận lợi cho việc cung cấp đa dạng các dịch vụ hữu ích đến với con người. Trong vài năm gần đây, nó không ngừng phát triển để phù hợp với một cộng đồng rộng lớn hơn nhiều, đem lại rất nhiều dịch vụ với các lợi ích thương mại, kinh tế, xã hội... Tuy nhiên, nó cũng trở thành môi trường cho các cuộc chiến tranh không gian số, nơi mà các cuộc tấn công của nhiều loại hình khác nhau (liên quan tài chính, tư tưởng, hành vi trả đũa...) đang được phát động. Các giao dịch thương mại điện tử được thực hiện trực tuyến là mối quan tâm chính của tội phạm mạng. Những hacker ăn cắp tài khoản của người dùng để thực hiện ý đồ xấu như mua bán trực tuyến, thỏa hiệp với một website hay máy chủ, phát động tấn công lên các hệ thống khác. Chính vì thế, hệ thống máy tính cần phải được bảo vệ khỏi các cuộc tấn công và phản ứng một cách thích hợp để tạo ra những xử lý nhằm giảm thiểu thiệt hại do tội phạm gây ra. Quá trình xử lý sự cố, phục hồi chứng cứ và truy tìm dấu vết tội phạm liên quan đến ngành khoa học điều tra số (digital forensics).

Phân tích điều tra mạng (Network Forensics) là một nhánh của ngành khoa học điều tra số đề cập đến việc chặn bắt, ghi âm và phân tích lưu lượng mạng cho mục đích điều tra và ứng phó sự cố. Có rất nhiều kỹ thuật cũng như công cụ hỗ trợ trong việc chặn bắt các dữ liệu lan truyền trên mạng để một cuộc tấn công hay một ý đồ xấu có thể bị điều tra, ngăn chặn. Công cụ hỗ trợ phân tích gói tin trong điều tra mạng là một vấn đề rất quan trọng và luôn cấp thiết. Để cho quá trình điều tra mạng được nhanh và chính xác thì một chương trình hỗ trợ cần phải được xây dựng một cách chính xác cung cấp nhiều thông tin cần thiết cho người điều tra.

Vì những lý do trên, nhóm đã chọn đề tài “**Theo dõi kẻ xâm nhập qua mạng**”.

# CHƯƠNG 1. TÌM HIỂU TỔNG QUAN VỀ ĐIỀU TRA MẠNG

## **Giới thiệu về điều tra số**

* + 1. *Khái niệm*

Điều tra số (đôi khi còn gọi là Khoa học điều tra số) là một nhánh của ngành Khoa học điều tra đề cập đến việc phục hồi và điều tra các tài liệu tìm thấy trong các thiết bị kỹ thuật số, thường có liên quan đến tội phạm máy tính. Thuật ngữ điều tra số ban đầu được sử dụng tương đương với điều tra máy tính nhưng sau đó được mở rộng để bao quát toàn bộ việc điều tra của tất cả các thiết bị có khả năng lưu trữ dữ liệu số.

Điều tra số có thể được định nghĩa là việc sử dụng các phương pháp, công cụ kỹ thuật khoa học đã được chứng minh để bảo quản, thu thập, xác nhận, chứng thực, phân tích, giải thích, lập báo cáo và trình bày lại những thông tin thực tế từ các nguồn kỹ thuật số với mục đích tạo điều kiện hoặc thúc đẩy việc tái hiện lại các sự kiện nhằm tìm ra hành vi phạm tội hay hỗ trợ cho việc dự đoán các hoạt động trái phép gây gián đoạn quá trình làm việc của hệ thống

* + 1. *Mục đích và ứng dụng*

Trong thời đại công nghệ phát triển mạnh như hiện nay. Song song với các ngành khoa học khác, điều tra số đã có những đóng góp rất quan trọng trong việc ứng cứu nhanh các sự cố xảy ra đối với máy tính, giúp các chuyên gia có thể phát hiện nhanh các dấu hiệu khi một hệ thống có nguy cơ bị xâm nhập, cũng như việc xác định được các hành vi, nguồn gốc của các vi phạm xảy ra đối với hết thống. Về mặt kỹ thuật thì điều tra số như: Điều tra mạng, điều tra bộ nhớ, điều tra các thiết bị điện thoại có thể giúp cho tổ chức xác định nhanh những gì đang xảy ra làm ảnh hưởng tới hệ thống, qua đó xác định được các điểm yếu để khắc phục, kiện toàn

Về mặt pháp lý thì điều tra số giúp cho cơ quan điều tra khi tố giác tội phạm công nghệ cao có được những chứng cứ số thuyết phục để áp dụng các chế tài xử phạt với các hành vi phạm pháp.

Một cuộc điều tra số thường bao gồm 3 giai đoạn: Tiếp nhận dữ liệu hoặc ảnh hóa tang vật, sau đó tiến hành phân tích và cuối cùng là báo cáo lại kết quả điều tra được.

Việc tiếp nhận dữ liệu đòi hỏi tạo ra một bản copy chính xác các sector hay còn gọi là nhân bản điều tra, của các phương tiện truyền thông, và để đảm bảo tính toàn vẹn của chứng cứ thu được thì những gì có được phải được băm sử dụng SHA1 hoặc MD5, và khi điều tra thì cần phải xác minh độ chính xác của các bản sao thu được nhờ giá trị đã băm trước đó.

Trong giai đoạn phân tích, thì các chuyên gia sử dụng các phương pháp nghiệp vụ, các kỹ thuật cũng như công cụ khác nhau để hỗ trợ điều tra. Sau khi thu thập được những chứng cứ có giá trị và có tính thuyết phục thì tất cả phải được tài liệu hóa lại rõ ràng, chi tiếp và báo cáo lại cho bộ phận có trách nhiệm xử lý chứng cứ thu được.

* 1. **Các loại hình điều tra phổ biến**
     1. *Điều tra máy tính*

Điều tra máy tính (Computer Forensics) là một nhánh của khoa học điều tra số liên quan đến việc phân tích các bằng chứng pháp lý được tìm thấy trong máy tính và các phương tiện lưu trữ kỹ thuật số như:

Điều tra bản ghi (Registry Forensics) là việc trích xuất thông tin và ngữ cảnh từ một nguồn dữ liệu chưa được khai thác qua đó biết được những thay đổi (chỉnh sửa, thêm bớt…) dữ liệu trong bản ghi (Register).

Điều tra bộ nhớ (Memory Forensics) là việc ghi lại bộ nhớ khả biến (bộ nhớ RAM) của hệ thống sau đó tiến hành phân tích làm rõ các hành vi đã xảy ra trên hệ thống. Để xác định các hành vi đã xảy ra trong hệ thống, người ta thường sử dụng kiến trúc quản lý bộ nhớ trong máy tính để ánh xạ, trích xuất các tập tin đang thực thi và cư trú trong bộ nhớ.

Điều tra phương tiện lưu trữ (Disk Forensics) là việc thu thập, phân tích dữ liệu được lưu trữ trên phương tiện lưu trữ vật lý, nhằm trích xuất dữ liệu ẩn, khôi phục các tập tin bị xóa, qua đó xác định người đã tạo ra những thay đổi dữ liệu trên thiết bị được phân tích.

Mục đích của điều tra máy tính là nhằm xác định, bảo quản, phục hồi, phân tích, trình bày lại sự việc và ý kiến về các thông tin thu được từ thiết bị kỹ thuật số. Mặc dù thường được kết hợp với việc điều tra một loạt các tội phạm máy tính, điều tra máy tính cũng có thể được sử dụng trong tố tụng dân sự. Bằng chứng thu được từ các cuộc điều tra máy tính thường phải tuân theo những nguyên tắc và thông lệ như những bằng chứng kỹ thuật số khác. Nó đã được sử dụng trong một số trường hợp có hồ sơ cao cấp và đang được chấp nhận rộng rãi trong các hệ thống tòa án Mỹ và Châu Âu

* + 1. *Điều tra mạng*

Điều tra mạng (Network Forensics) là một nhánh của khoa học điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập. Điều tra mạng cũng được hiểu như điều tra số trong môi-trường-mạng. Điều tra mạng là một lĩnh vực tương đối mới của khoa học pháp y. Sự phát triển mỗi ngày của Internet đồng nghĩa với việc máy tính đã trở thành mạng lưới trung tâm và dữ liệu bây giờ đã khả dụng trên các chứng cứ số nằm trên đĩa. Điều tra mạng có thể được thực hiện như một cuộc điều tra độc lập hoặc kết hợp với việc phân tích pháp y máy tính (computer forensics) thường được sử dụng để phát hiện mối liên kết giữa các thiết bị kỹ thuật số hay tái tạo lại quy trình phạm tội.

* + 1. *Điều tra thiết bị di động*

Điều tra thiết bị di động (Mobile device Forensics) là một nhánh của khoa học điều tra số liên quan đến việc thu hồi bằng chứng kỹ thuật số hoặc dữ liệu từ các thiết bị di động. Thiết bị di động ở đây không chỉ đề cập đến điện thoại di động mà còn là bất kỳ thiết bị kỹ thuật số nào có bộ nhớ trong và khả năng giao tiếp, bao gồm các thiết bị PDA, GPS và máy tính bảng.

Việc sử dụng điện thoại với mục đích phạm tội đã phát triển rộng rãi trong những năm gần đây, nhưng các nghiên cứu điều tra về thiết bị di động là một lĩnh vực tương đối mới, có niên đại từ những năm 2000. Sự gia tăng các loại hình điện thoại di động trên thị trường (đặc biệt là điện thoại thông minh) đòi hỏi nhu cầu giám định các thiết bị này mà không thể đáp ứng bằng các kỹ thuật điều tra máy tính hiện tại.

# CHƯƠNG 2. THEO DÕI KẺ XÂM NHẬP TRÊN MẠNG

* 1. **Tìm hiểu về hệ thống phát hiện xâm nhập**

Kẻ xâm nhập vào hệ thống mạng chính là cơn ác mộng tồi tệ nhất của bất kỳ quản trị viên mạng nào. Các cuộc khảo sát được thực hiện bởi hầu hết các tổ chức đáng tin cậy nhất trên thế giới đều chỉ ra rằng khi nói đến xâm nhập mạng, vấn đề không phải nếu là mạng bị xâm phạm, mà là vấn đề khi nào mạng bị vi phạm. Một số trang web và hệ thống mạng nổi tiếng đã từng bị tấn công trong quá khứ bao gồm Lầu năm góc, NATO, Nhà trắng, v.v. Là một nhà điều tra mạng, điều quan trọng là phải hiểu các cách thức và vai trò của việc phát hiện và ngăn chặn xâm nhập.

Có rất nhiều hệ thống phát hiện/ngăn chặn xâm nhập. Nó có thể là host-based IDS/IPS (Hệ thống phát hiện xâm nhập máy chủ) hoặc network-based IDS/IPS (Hệ thống phát hiện xâm nhập mạng) . Các hệ thống phát hiện xâm nhập máy chủ giám sát hoạt động của máy chủ lưu trữ, trong khi các hệ thống phát hiện xâm nhập mạng giám sát hoạt động dựa trên việc thu thập và phân tích lưu lượng mạng.

Chương này sẽ tập trung vào việc phát hiện/ngăn chặn xâm nhập bằng cách sử dụng hệ thống phát hiện xâm nhập mạng (NIDS) và Hệ thống ngăn chặn xâm nhập mạng (NIPS). Chúng ta sẽ đánh giá chức năng của từng hệ thống và so sánh sự khác biệt giữa chúng.

### *2.1.1.Tổng quan về hệ thống phát hiện xâm nhập*

Hệ thống phát hiện xâm nhập mạng (NIDS) khá giống với hệ thống báo động cảnh báo sớm mà chúng ta thấy trong các bộ phim vượt ngục. Chúng được kích hoạt bởi một sự kiện được xác định trước (chẳng hạn như một lần đột nhập vào/ra) được xác định dựa trên một quy tắc được thiết lập bởi quản trị viên/điều tra viên. Giống như một thiết bị báo trộm trong nhà, NIDS được thiết kế để phát hiện ra kẻ đột nhập và đưa ra cảnh báo cho người được ủy quyền.

Thông thường, NIDS có thể phát hiện các xâm nhập trong segment mạng mà nó đang theo dõi. Điểm mấu chốt tác động tới hiệu quả của nó là vị trí đặt thiết bị NIDS chính xác để cho phép giám sát tất cả lưu lượng truy cập mạng vào và ra khỏi hệ thống. Có một cách đó là đặt nó trên mạng và để phản chiếu lưu lượng tin đi qua nó. Điều này được thực hiện để đảm bảo tất cả lưu lượng truy cập mạng đi qua thiết bị NIDS.

NIDS sẽ giám sát tất cả lưu lượng truy cập từ cả bên trong ra lẫn bên ngoài vào và xác định các cuộc xâm nhập bằng cách phát hiện các mẫu bất thường trong lưu lượng mạng. Điều này được thực hiện bằng cách xác định bất kỳ các dấu hiệu đặc biệt của các cuộc xâm nhập hoặc tấn công được tìm thấy trong lưu lượng truy cập bị chặn. Một hệ thống IDS điển hình về cơ bản là một hệ thống thụ động, nắm bắt lưu lượng truy cập, kiểm tra các gói tin, so sánh nội dung với các dấu hiệu xấu đã biết và đưa ra các cảnh báo tương ứng. Điều này được mô tả trong hình ảnh sau đây:

Một IDS điển hình duy trì một cơ sở dữ liệu lớn về các dấu hiệu đặc trưng của một cuộc tấn công. Chúng có thể đại diện cho các cuộc xâm nhập đã cố gắng hoặc thực tế, vi rút hoặc worm. Trong quá trình hoạt động, IDS sẽ xem xét tất cả lưu lượng truy cập mạng và so sánh nó với cơ sở dữ liệu về các dấu hiệu đã biết. Vì vậy, bất kỳ IDS nào cũng tốt như chất lượng của cơ sở dữ liệu chữ ký của nó. Một cơ sở dữ liệu chất lượng tốt sẽ tạo ra ít False Positive và có giá trị cao.

Sau đây là bảng liệt kê loại trạng thái cảnh báo của NIDS:

|  |  |  |  |
| --- | --- | --- | --- |
| **Loại** | **Sự kiện** | **Hành động** | **Mô tả** |
| True Positive | Tấn công | Cảnh báo | Một cuộc tấn công thực sự và gây ra một báo động |
| False Positive | Không tấn công | Cảnh báo | Báo động được kích hoạt trong khi không có cuộc tấn công nào xảy ra |
| False Negative | Tấn công | Không cảnh báo | Một cuộc tấn công thực sự xảy ra nhưng không có báo động |
| True Negative | Không tấn công | Không cảnh báo | Khi không có cuộc tấn công nào và không có báo động |

*Bảng 2. 1. Bảng liệt kê các trạng thái cảnh báo của NIDS*

Như chúng ta có thể thấy từ bảng trên, cả False Positive và False Negative là những yếu tố rất đáng quan tâm.

Một thông báo False Positive chiếm các tài nguyên có giá trị để giải quyết xem cảnh báo đó có chính xác không. Do đó, một số lượng lớn các cảnh báo False Positive có thể hoàn toàn làm giảm sự tin cậy của IDS, khiến các cảnh báo True Positive bị bỏ qua và gây ra nhiều tác hại. Một tình huống *Cry Wolf* điển hình!

False Negative là mối vấn đề nghiêm trọng hơn. Khi một cuộc tấn công diễn ra một cách bí mật mà không được chú ý tới, sẽ mất rất nhiều thời gian để khám phá và cuối cùng thì, mức độ ảnh hưởng sẽ tăng lên đáng kể. Điều này có thể gây ra tổn thất lớn cho một tổ chức.

*2.1.2. Tìm hiểu về hệ thống ngăn chặn xâm nhập mạng*

Trong phần trước, chúng ta đã dành thời gian để hiểu NIDS. Điều này giúp chúng ta có một nền tảng vững chắc khi tiếp tục tìm hiểu về NIPS.

Không giống như NIDS, là một hệ thống thụ động, NIPS là một hệ thống hoạt động giám sát lưu lượng mạng và thực hiện hành động phòng ngừa ngay lập tức khi phát hiện ra mối đe dọa. Sự xâm nhập thường được theo dõi rất nhanh dựa trên các hành vi khai thác lỗ hổng. Chúng thường ở dạng tiêm dữ liệu độc hại vào một ứng dụng hoặc dịch vụ với mục tiêu làm gián đoạn và giành quyền kiểm soát thiết bị hoặc ứng dụng. Điều này có thể dẫn đến việc DoS – từ chối dịch vụ (vô hiệu hóa các ứng dụng hoặc dịch vụ), lạm dụng đặc quyền hoặc leo thang để lạm dụng và giành quyền kiểm soát hệ thống hoặc tài nguyên.

Trong thế giới bảo mật thông tin, hầu hết các khai thác đều có ngày hết hạn. Điều này là do thời điểm khai thác đã được xác định, các nhà cung cấp phần mềm sẽ cập nhật các bản vá, các nhà cung cấp sản phẩm bảo mật IDS/IPS/bảo mật dựa trên dấu hiệu vi phạm sẽ nhanh chóng xác định và khắc phục nó, và mọi quản trị viên mạng đều có các cách thức riêng để bảo vệ mạng của mình khỏi một cuộc tấn công.

Do đó, chúng ta thấy rằng trừ khi một lỗ hổng cụ thể được khai thác nhanh chóng, nó sẽ không thể sử dụng được như một vectơ tấn công. Do đó, với những kẻ xâm nhập, thời gian là điều cốt yếu. Trong tình huống như vậy, NIPS đóng một vai trò quan trọng trong hệ thống phòng thủ của mạng.

Thông thường, NIPS được đặt trực tiếp phía sau tường lửa đối diện với mạng Internet. Vì đây là nội tuyến, nó chủ động phân tích tất cả lưu lượng truy cập mạng và tự động loại bỏ các gói có nội dung độc hại.

*Một số tác vụ của NIPS:*

* Thông báo cho quản trị viên về sự kiện gây ra cảnh báo; tương tự với NIDS
* Loại bỏ các gói tin độc hại đã xác định
* Chấm dứt các kết nối và chặn địa chỉ IP nguồn
* Reset lại kết nối

*Một số lĩnh vực chính mà NIPS phải giải quyết:*

* An ninh mạng (chức năng quan trọng để chống lại các mối đe dọa và False Positive)
* Hiệu suất của mạng (phòng chống sự suy giảm hiêu suất của mạng bằng cách làm việc hiệu quả và nhanh chóng)
  1. **Phương thức phát hiện**

NIDS và NIPS sử dụng các phương pháp khác nhau để phát hiện sự xâm nhập. Hai phương pháp phát hiện phổ biến nhất là so trùng mẫu (Pattern matching) và phát hiện dấu hiệu bất thường (Anomaly detection).

### *2.2.1. So trùng mẫu (Pattern matching)*

Phát hiện kẻ xâm nhập bằng cách sử dụng so trùng mẫu (pattern matching) cũng được gọi là phát hiện sử dụng sai (misuse detection) hoặc phát hiện dựa trên dấu hiệu (signature-based detection). Về cơ bản, cách thức này được sử dụng để phát hiện các cuộc tấn công đã biết dựa trên các mẫu của chúng bao gồm các hành động cụ thể xảy ra như một phần của cuộc tấn công hay được biết đến là “signature” - dấu hiệu đặc trưng.

Điều này tương tự như việc xác định tội phạm từ dấu vân tay mà họ để lại tại hiện trường vụ án. Tuy nhiên, để có thể xác định chính xác danh tính của tên tội phạm có mặt tại hiện trường vụ án, chúng ta cần phải có dấu vân tay của anh ấy/cô ấy trong cơ sở dữ liệu của mình. Tương tự như vậy, chúng ta cần phải có mẫu hoặc các dấu hiệu đặc trưng của các cuộc tấn công có trong cơ sở dữ liệu của mình thì IDS/IPS mới có thể bắt được một sự kiện như vậy.

Do đó, hiệu quả của IDS dựa trên so trùng mẫu (pattern matching) hoàn toàn phụ thuộc vào cơ sở dữ liệu. Do đó với loại IDS này, điều quan trọng là phải giữ cho cơ sở dữ liệu các dấu hiệu đặc trưng luôn luôn được cập nhật.

Đây cũng chính là điểm yếu lớn nhất của so trùng mẫu (pattern matching). Trừ khi thông tin của cuộc tấn công có mặt trong cơ sở dữ liệu, nó sẽ không được phát hiện và sẽ dễ dàng triển khai thành công. Do đó, tính nhạy cảm của mạng đối với các cuộc tấn công *Zero day* hoặc các hình thức tấn công mới là khá cao. Ngoài ra, một số cuộc tấn công dựa trên mã độc phổ biến sẽ khai thác điểm yếu này. Chúng sẽ thực hiện một sửa đổi nhỏ trong mẫu để vượt qua so trùng mẫu (pattern matching), thứ mà tìm kiếm các dấu hiệu nhận biết cụ thể. Do đó, ngay cả một cuộc tấn công cùng loại, các dấu hiệu sẽ được thay đổi sẽ khiến NIDS và NIPS không thể phát hiện ra nó.

### *2.2.2. Dấu hiệu bất thường (anomaly detection)*

Phát hiện dựa trên dấu hiệu bất thường là việc so sánh thống kê của các kiểu sử dụng thông thường với sự khác biệt gây ra bởi các cuộc tấn công.

Để bắt đầu, một hồ sơ cơ sở được thiết lập để xác định điều gì là *bình thường*. Tiếp theo, các hành động bên ngoài các tham số *bình thường* sẽ được theo dõi. Theo cách này, chúng ta có thể bắt được bất kỳ kẻ xâm nhập mới nào trên mạng mà phương thức tấn công của chúng không có dấu hiệu đặc trưng nào của một cuộc tấn công đã biết trong cơ sở dữ liệu NIDS.

Điều này tương tự như một người bảo vệ ban đêm bảo vệ một khu vực cụ thể. Anh ta biết từ kinh nghiệm những gì là bình thường cho khu vực. Bất cứ điều gì anh ta thấy bất bình thường này sẽ là cơ sở cho sự nghi ngờ từ phía anh ta.

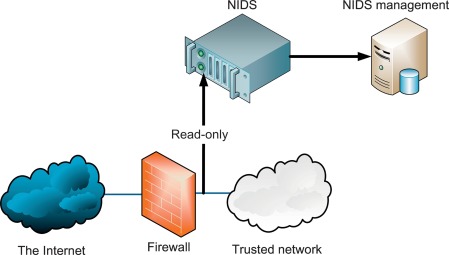
Một vấn đề lớn với IDS dựa trên phát hiện bất thường là tỷ lệ False Positive cao. Điều này là do bất kỳ hành vi nào có vẻ bất thường sẽ được xác định là một cuộc tấn công vào mạng.

Ngoài ra, IDS dựa trên sự bất thường là tỷ lệ False Positive cao hơn bởi vì hành vi không bình thường sẽ được gắn cờ là một cuộc tấn công có thể xảy ra, ngay cả khi nó không có. Điều này có thể được giảm nhẹ một phần bằng phương pháp phỏng đoán tiên tiến và học máy.

* 1. **Phân biệt giữa NIDS và NIPS**

Thoạt nhìn, cả hai giải pháp có vẻ khá giống nhau; tuy nhiên, có một sự khác biệt rõ ràng ở chỗ đó là một hệ thống giám sát và phát hiện thụ động, tự giới hạn việc đưa ra cảnh báo dựa trên một dấu hiệu bất thường, và một hệ thống phòng ngừa chủ động thực hiện hành động khi phát hiện gói độc hại bằng cách loại bỏ nó.

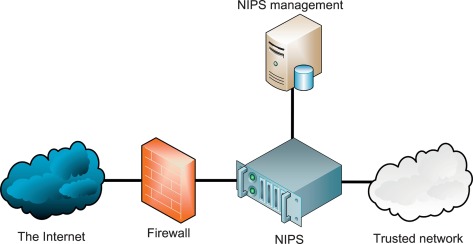
Thông thường, một NIPS là nội tuyến (giữa tường lửa và phần còn lại của mạng) và thực hiện hành động chủ động dựa trên bộ quy tắc được cung cấp cho nó. Trong trường hợp của NIDS, thiết bị/máy tính thường không phải là nội tuyến nhưng có thể nhận được từ một cổng đường mạng hoặc mirror port.



*Hình 2. 1. Mô hình NIDS*

Như bạn đã thấy ở hình trên, NIDS thường được đặt ở trước firewall. NIDS sẽ phát hiện các cuộc tấn công hoặc các bất thường về traffic mạng sau đó thông báo cho quản trị viên nếu chúng xảy ra và bên trong, firewall sẽ làm nhiệm vụ ngăn chặn những tấn công xâm nhập này. Tuy nhiên, NIDS cũng có thể được đặt sau firewall hoặc có thể được đặt ở nhiều điểm quan trọng trong mạng. Bất kể vị trí đặt NIDS, quản trị hệ thống nên giám sát traffic nhiều lần…để làm được điều này, máy tính hoặc server mà NIDS được cài đặt cần phải có một card mạng được cấu hình ở chế độ promiscuous.

Bạn cần lựa chọn kết hợp giữa NIDS và HIDS sao cho hợp lý. Vì điểm bất lợi của NIDS là nó không có khả năng đọc được các gói thông tin đã được mã hóa và nó cũng không thể phát hiện được các vấn đề xảy ra trên máy tính cá nhân. Vì vậy, để an toàn cho cả mạng lẫn các máy tính cá nhân, một số tổ chức đã kết hợp giữa NIDS và HIDS. Nếu NIDS được đặt trước firewall thì nó sẽ là đối tượng để tấn công, vì vậy nó cần được giám sát và cập nhật thường xuyên. Một số NIDS có chức năng cập nhật tự động. cuối cùng, nhược điểm lớn nhất của NIDS là nó chỉ có thể phát hiện các cuộc tấn công. Để bảo vệ, ngăn chặn các cuộc tấn công, bạn cần một NIPS.



*Hình 2. 2. Mô hình NIPS*

Một hệ thống ngăn chặn xâm nhập được thiết kế để kiểm tra traffic dựa trên các cấu hình hoặc chính sách bảo mật, nó có thể loại bỏ, giữa lại hoặc chuyển hướng các mối đe dọa về traffic. Càng ngày càng có nhiều công ty cung cấp giải pháp NIPS thay vì NIDS. Ví dụ Enterasys Intrusion Prevention System (còn gọi là Dragon IPS), Check Point Security Applicances, McAfee IntruShield …NIPS không chỉ loại bỏ hoặc chuyển hướng traffic mà nó còn chuyển hướng đến một vùng được gọi là padded cell khi phát hiện ra kẻ tấn công. Padded cell là một vùng đệm và đặc biệt hơn nó không chứa bất cứ thông tin nào có giá trị cũn như không có lối ra.

Giống như NIDS, NIPS thường được đặt trước firewall mặc dù bạn có thể đặt nó ở nơi khác tùy thuộc vào kiến trúc và sơ đồ mạng của bạn.. Theo giải pháp mà bạn chọn, các gói dữ liệu sẽ đi qua các thiết bị và nó sẽ được kiểm tra. Những thiết bị NIPS cần có tính chính xác cao cũng như cập nhật thường xuyên để tránh những sự cố xác định và ngăn chặn nhầm. Một số NIPS có thể giám sát các signature và các dấu hiệu bất thường. Một số lỗi có thể xảy ra với NIDS và NIPS và nó có thể phá vỡ các hệ thống này. Tấn công như thế nào? Kẻ tấn công sẽ lợi dụng việc các lỗi xác định sai mà từ từ tấn công vào mạng vì phần mềm cũng do con người tạo nên. Để chống lại điều này, một số thiết bị có khả năng che giấu IP để tránh bị tấn công. Chúng cũng được kết nối với firewall nội bộ. Và cuối cùng là bạn nên chọn giải pháp IPS sao cho khu vực quản lý được an toàn vì nếu kẻ tấn công làm chủ được khu vực quản lý thì hệ thống mạng của bạn có nguy cơ bị xâm nhập.

NIPS có thể bảo vệ không chỉ máy tính mà còn các thiết bị mạng như switch, router và firewall. Ngoài ra, NIPS còn có khả năng như một bộ máy phân tích giao thức bằng cách đọc các traffic đã được mã hóa hoặc ngăn chặn các cuộc tấn công đã được mã hóa.

Như đã nói, NIDS hay NIPS cần có tính chính xác cao và cập nhật thường xuyên để ngăn phòng ngừa việc nhận dạng sai (misidentification) traffic mạng hoặc tệ hơn là các cuộc tấn công. Có 2 loại misidentification mà bạn cần biết:

* **False positive**: khi một người dùng không có quyền truy cập vẫn có thể truy cập vào được hệ thống thì được gọi là false positive.
* **False negative** – khi một người có quyền truy cập nhưng bị ngăn chặn truy cập thì được gọi là false negative

Chi phí thiết lập mạng trong trường hợp của NIPS tốn nhiều hơn NIDS.

Một vấn đề khác với NIDS là vào thời điểm kẻ xâm nhập vào hệ thống và thông báo của quản trị viên, kẻ xâm nhập đã xâm nhập hệ thống ở mức độ sâu hơn, do đó làm cho một tình huống cực xấu xảy ra một cách đơn giản.

Mặc dù tính ổn định là tối quan trọng trong cả hai hệ thống, hậu quả của việc NIDS gặp sự cố là một điểm mù trong an ninh mạng trong thời gian nó ngừng hoạt động. Tuy nhiên, trong trường hợp NIPS gặp sự cố, toàn bộ mạng có thể bị ảnh hưởng nghiêm trọng.

IDS có thể được sử dụng trong chế độ chủ động và điều này có sẽ làm giảm đi sự khác biệt giữa IPS và IDS chủ động. IDS chủ động có thể được cấu hình để loại bỏ các gói dựa trên các tiêu chí nhất định hoặc thậm chí chuyển hướng lưu lượng truy cập qua một thiết bị mạng.

Ngày nay, chúng ta thường thấy sự sử dụng chồng chéo giữa tường lửa, NIPS và NIDS. Trong thực tế, đôi khi các nhà sản xuất đã kết hợp tất cả những thứ này vào một sản phẩm duy nhất điển hình là một số thiết bị quản lý mối đe dọa hợp nhất (Unified Threat Management-UTM) hiện có sẵn trên thị trường.

* 1. **Sử dụng Snort để phát hiện, ngăn chặn xâm nhập mạng**

*2.4.1. Giới thiệu*

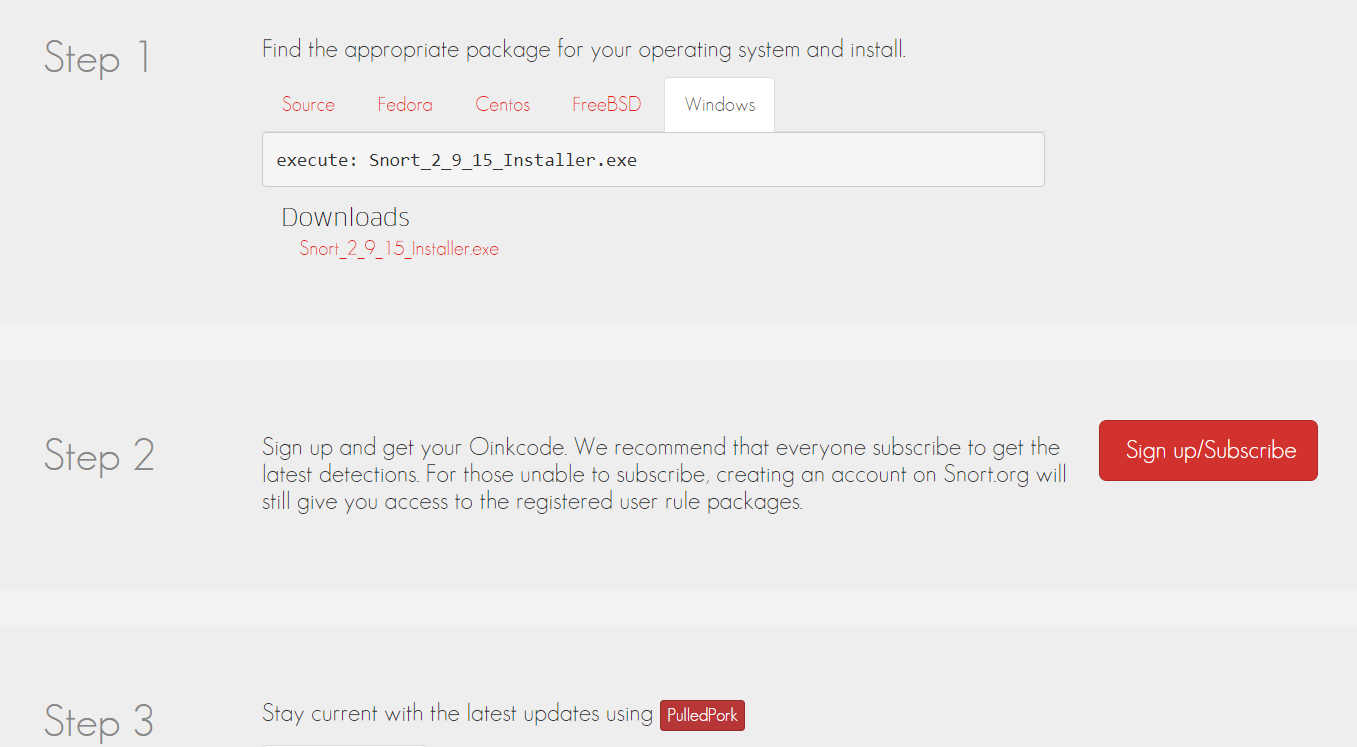
SNORT là một hệ thống phát hiện/ngăn chặn xâm nhập mã nguồn mở có khả năng phân tích lưu lượng thời gian thực và ghi nhật ký gói tin. SNORT được sử dụng một cách vô cùng phổ biến, là công cụ được lựa chọn cho cộng đồng mã nguồn mở. Mặc dù có một số NIDS và NIPS, chúng ta sẽ chỉ tập trung với SNORT ở chương này.

Bên cạnh việc có thể hoạt động như một ứng dụng thu bắt gói tin thông  
thường, Snort còn có thể được cấu hình để chạy như một NIDS. Snort hỗ trợ  
khả năng hoạt động trên các giao thức sau: Ethernet, 802.11, Token Ring,  
FDDI, Cisco HDLC, SLIP, PPP, và PF của OpenBSD.

Trang web của SNORT <https://www.snort.org/>:

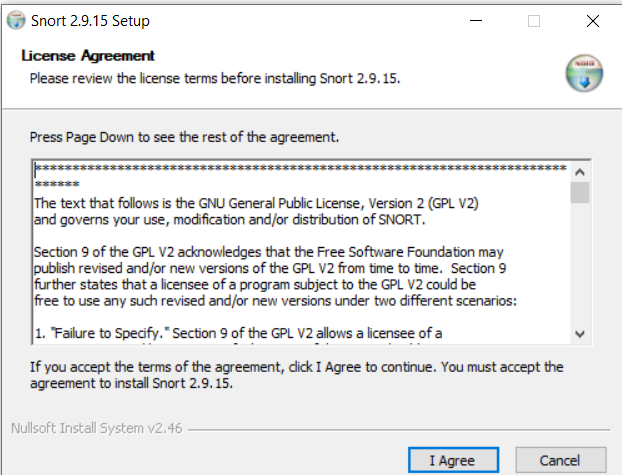
Rất dễ dàng để xem qua các tài liệu có sẵn trên trang web vì thông tin này được cập nhật trên website khá thường xuyên. Tại thời điểm viết bài, SNORT có sẵn các phiên bản chạy trên một số bản phân phối Linux cũng như Windows. Liên kết tải xuống sẽ hướng dẫn chúng tôi thực hiện chính xác các bước cài đặt.

### *2.4.2. Sử dụng snort để phát hiện, ngăn chặn xâm nhập mạng*



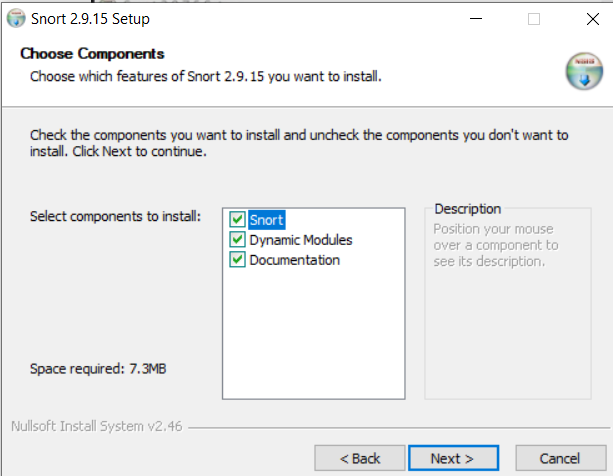
*Hình 2. 3. Thiết lập snort trên windows 1*

Sau khi tải xuống, chúng tôi cần cài đặt SNORT theo quy trình sau:



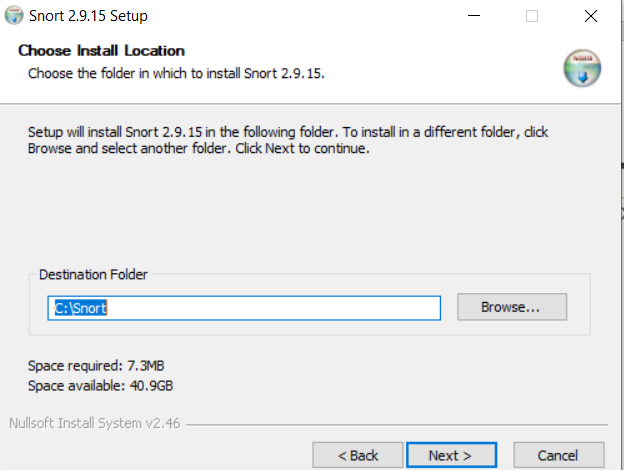
*Hình 2. 4. Thiết lập snort trên windows 2*

Chúng tôi bắt đầu bằng cách đồng ý với Giấy phép Công cộng GNU (GPL) để chúng tôi có thể tiến hành cài đặt SNORT:

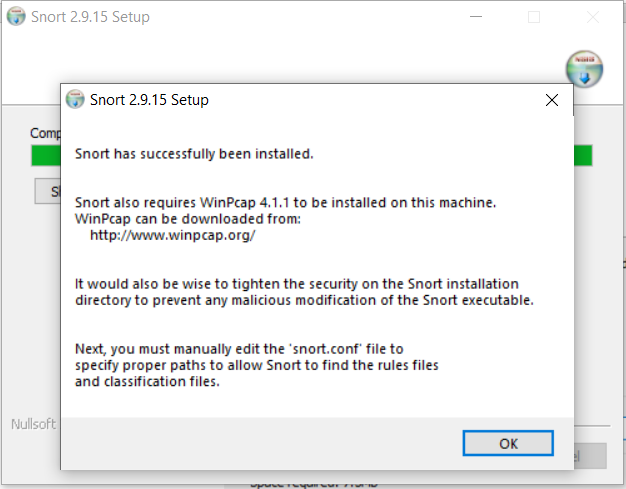


*Hình 2. 5. Thiết lập snort trên windows 3*

Sau đó chúng tôi tiến hành chọn các thành phần mà chúng tôi cần và chúng tôi đã hoàn thành:

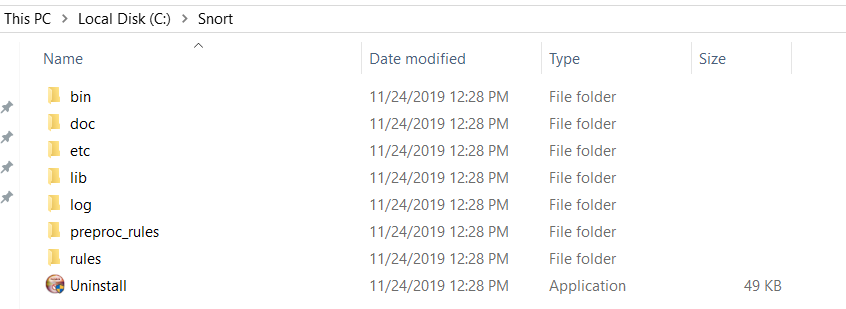


*Hình 2. 6. Thiết lập snort trên windows 4*



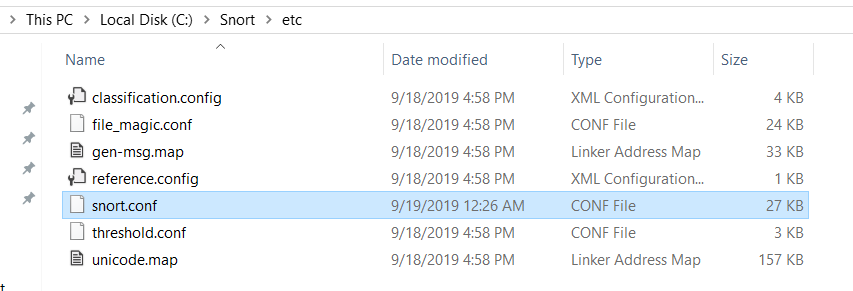
*Hình 2. 7. Thiết lập snort trên windows 5*

Bước quan trọng cần thực hiện sau đó là chỉnh sửa tệp snort.conf, nơi chúng tôi có thể chỉ định các đường dẫn thích hợp cho SNORT để tìm hướng dẫn:

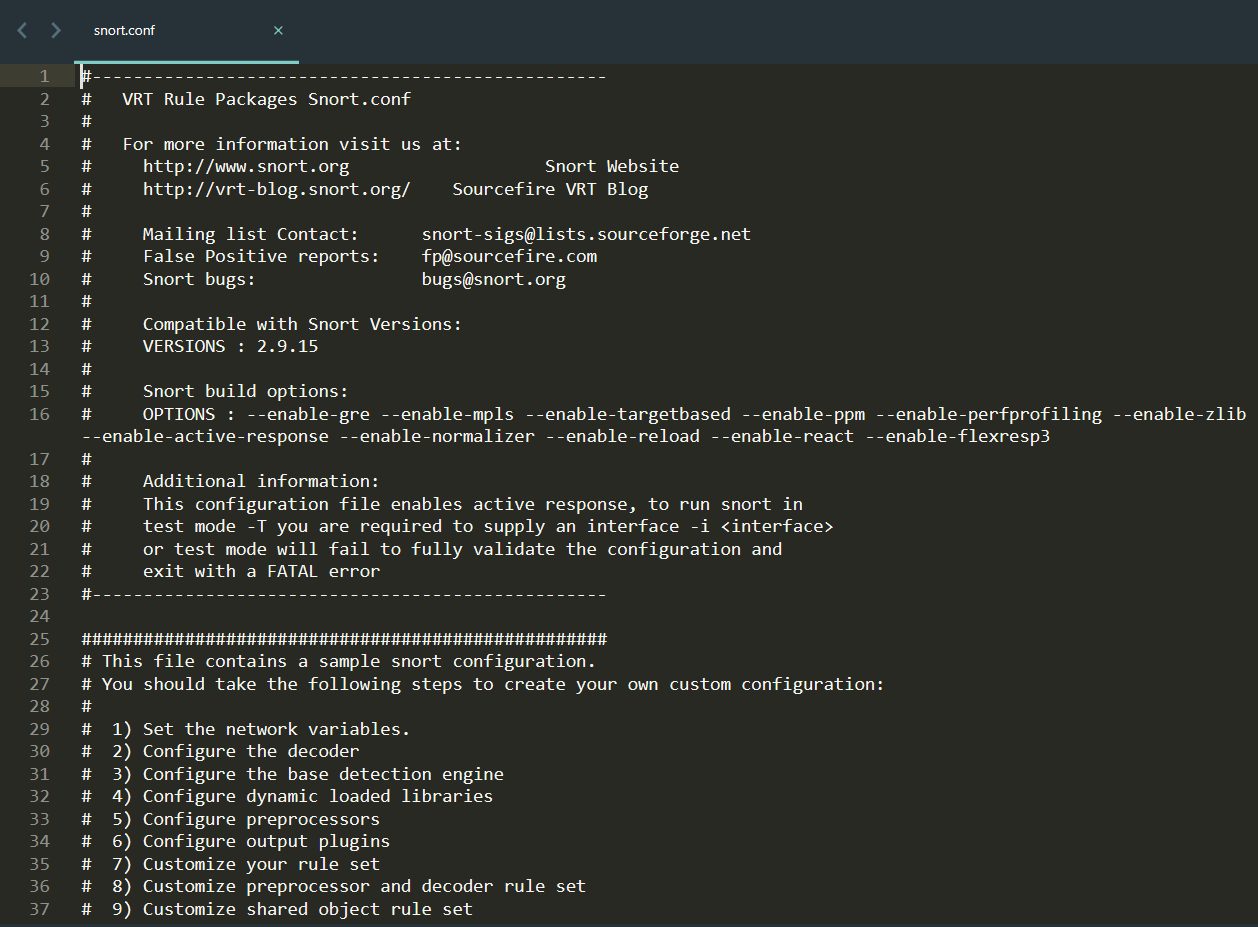


*Hình 2. 8. Thiết lập snort trên windows 6*

Sử dụng trình chỉnh sửa tệp văn bản như Notepad (dành cho Windows) hay nano cho Linux được sử dụng để chỉnh sửa tệp snort.conf:



*Hình 2. 9. Thiết lập snort trên windows 7*



*Hình 2. 10. Thiết lập snort trên windows 8*

SNORT có thể được cấu hình để chạy ở ba chế độ:

* Chế độ sniffer
* Chế độ ghi nhật ký gói
* Chế độ phát hiện / ngăn chặn xâm nhập mạng

**Chế độ sniffer**

Chế độ sniffer chỉ đọc các gói và hiển thị chúng trong chế độ giao diện console.Để bắt đầu, chúng tôi sử dụng lệnh sau:

***./snort –v***

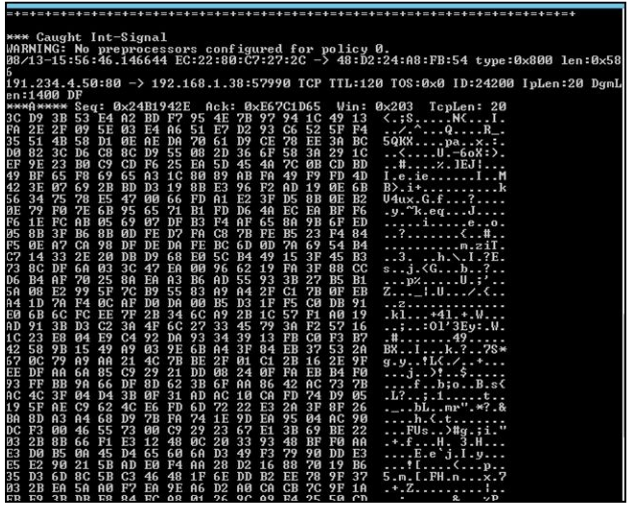
Điều này chạy SNORT ở chế độ verbose, hiển thị IP, lấy các tiêu đề gói TCP /IP/UDP/ICMP và in chúng ra màn hình.

Trong khi --v hiển thị chi tiết về các tiêu đề gói, chúng tôi có thể cảm thấy cần phải xem nội dung gói. Để xem những điều này, chúng ta cần gõ lệnh sau: ***snort –vd***

Để biết chi tiết với các tiêu đề lớp liên kết dữ liệu mở rộng, chúng ta có thể sử dụng lệnh sau:

***snort –vde***

Sau đây là đầu kết quả cho lệnh trước:

**

*Hình 2. 11. Kết quả câu lệnh 1*

**Chế độ ghi nhật ký gói**

Chế độ logger gói tương tự như chế độ sniffer, ngoại trừ việc nó ghi các gói vào đĩa. Để cho phép nó thực hiện điều này, chúng ta cần thiết lập thư mục chụp, trong đó SNORT sẽ lưu trữ các gói đã bắt.

Theo mặc định, cài đặt SNORT tạo một thư mục nhật ký trong thư mục snort. Chúng tôi có thể sử dụng thư mục này cho mục đích lưu trữ các gói chụp. Lệnh cho việc này như sau:

**./snort –vde –l ./log**

Trong trường hợp này, chúng tôi đang yêu cầu SNORT nắm bắt các tiêu đề, gói và thông tin lớp liên kết dữ liệu từ tất cả các gói và lưu trữ chúng trong một thư mục được chỉ định ở định dạng nhật ký.

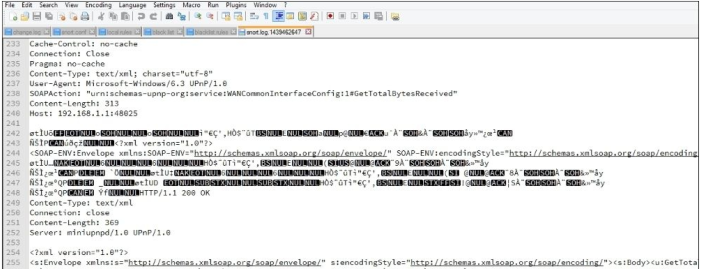
Để cho phép ghi nhật ký liên quan đến mạng gia đình của chúng tôi, chúng tôi cũng có thể chỉ định SNORT mạng gia đình bằng cách sử dụng phạm vi và dải địa chỉ IP của mạng, ví dụ: 192.168.1.0/24.

Tuy nhiên, nếu chúng ta sẽ cần phải xem và phân tích các gói sau này trong một trình thám thính khác như Wireshark, thì chúng ta cần thực hiện việc chụp hoặc đăng nhập ở chế độ nhị phân. Để làm điều này, chúng tôi sử dụng lệnh sau:

**./snort –l ./log –b**

SNORT cũng có khả năng đọc lại các gói này bằng cách sử dụng bộ chuyển đổi, điều này đặt nó ở chế độ phát lại.

Dưới đây là tệp nhật ký mẫu được tạo bằng tùy chọn đầu tiên:

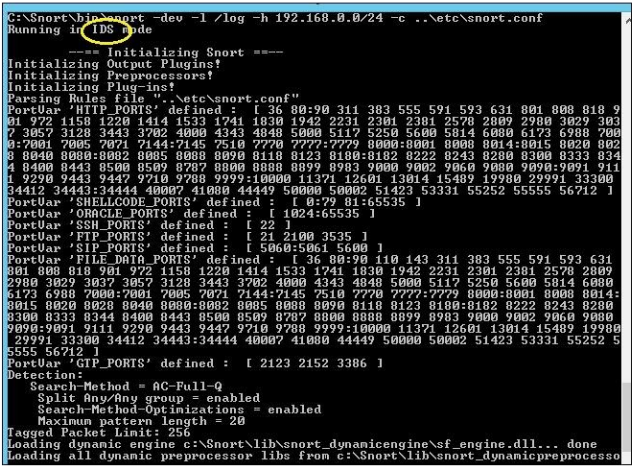


*Hình 2. 12. Kết quả câu lệnh 2*

**Chế độ phát hiện / ngăn chặn xâm nhập mạng**

Chìa khóa cho việc sử dụng hiệu quả SNORT cho mục đích phát hiện xâm nhập hoặc ngăn chặn xâm nhập là tệp cấu hình SNORT thường được gọi là tệp snort.conf.

Lệnh bắt đầu nhanh trong chế độ NIDS cơ bản như sau:



*Hình 2. 13. Kết quả câu lệnh 3*

SNORT có thể chạy ở ba chế độ khác nhau:

* **Thụ động:** Đây là chế độ mặc định và SNORT hoạt động như một NIDS trong chế độ này. Đây còn được gọi là chế độ TAP. Các luật drop không được sử dụng

**Nội tuyến:** Đây là chế độ hoạt động và SNORT hoạt động như một NIPS trong vai trò này. Điều này cho phép các luật drop được kích hoạt.

* **Kiểm tra nội tuyến**: Chế độ này mô phỏng chế độ nội tuyến của SNORT, do đó cho phép đánh giá hành vi nội tuyến mà không ảnh hưởng đến lưu lượng và hiệu suất.

Điều đặc biệt thực sự của SNORT nằm trong quy tắc. Dựa trên các quy tắc, SNORT có thể được cấu hình để đưa ra cảnh báo hoặc thực hiện hành động cụ thể.

Cảnh báo có thể ở dạng sau:

* Kết quả ở dạng màn hình console hoặc màn hình có giao diện
* Kết quả cho một tệp nhật ký
* Kết quả cho cơ sở dữ liệu SQL
* Kết quả ở dạng nhị phân để sử dụng với các trình thám thính khác
* E-mail cho một quản trị viên

Các quy tắc SNORT được chia thành hai phần logic. Tùy chọn các luật và tiêu đề các luật:

* Tiêu đề các luật bao gồm các địa chỉ IP hành động, giao thức, nguồn và đích và thông tin mạng và thông tin cổng nguồn và đích
* Phần tùy chọn các luật chứa thông tin và thông báo cảnh báo trên cơ sở các phần của gói cần được kiểm tra để xác định xem có nên thực hiện hành động theo luật không

*Các tùy chọn hành động các luật như sau:*

* **Alert**: Điều này tạo ra một cảnh báo dựa trên phương pháp đã chọn và sau đó ghi nhật ký gói
* **Drop:** Điều này chặn và ghi nhật ký gói
* **Pass:** Cái này chỉ bỏ qua gói
* **Log:** Đây chỉ là ghi nhật ký gói
* **Sdrop:** Cái này chỉ chặn gói và không ghi nhật ký
* **Reject:** Điều này chặn và ghi nhật ký gói, sau đó gửi thiết lập lại TCP cho giao thức TCP hoặc thông báo không thể truy cập cổng ICMP nếu giao thức là UDP
* **Active**: Điều này sẽ gửi một cảnh báo, sau đó bật chế độ động
* **Dynamic:** Điều này không hoạt động cho đến khi được kích hoạt bởi quy tắc kích hoạt và sau đó hoạt động như một quy tắc nhật ký

Chúng ta cũng có thể xác định các loại quy tắc của riêng mình và liên kết một hoặc nhiều plugin đầu ra cho chúng. SNORT hiện đang phân tích các giao thức TCP, UDP, ICMP và IP.

Làm cho các quy tắc được minh họa tốt hơn bằng một ví dụ. Hãy để Giả sử rằng chúng ta muốn cảnh báo cho quản trị viên về tất cả các nỗ lực của kẻ xâm nhập để telnet (Cổng 23) vào mạng của chúng ta..

Vì lợi ích của cuộc thảo luận của chúng tôi, hãy để nói rằng mạng gia đình của chúng tôi có dải IP từ 192.168.1.0 đến 255. Trong trường hợp như vậy, chúng tôi sẽ viết quy tắc sau:

***alert tcp any any -> 192.168.1.0/24 23***

Điều này có nghĩa là mọi nỗ lực từ bất kỳ mạng và bất kỳ cổng nào để telnet vào mạng gia đình 192.168.1.0/24 của chúng tôi sẽ tạo ra cảnh báo xâm nhập cho quản trị viên mạng. Điều này sẽ cho thấy một kẻ xâm nhập đang cố gắng telnet vào mạng của chúng tôi.

Tuy nhiên, vì chúng tôi muốn cảnh báo sẽ dài dòng một chút và giải thích nỗ lực của kẻ xâm nhập bằng ngôn ngữ đơn giản, chúng tôi sẽ sử dụng phần tùy chọn quy tắc và thêm một số thông tin bổ sung, như sau:

***alert tcp any any -> 192.168.1.0/24 23 (msg:"Intruder Alert – Telnet used"; flags:A+;classtype:policy-violation;sid:100001;rev:1;)***

Trong trường hợp này, thông báo Intruder Alert - Telnet used sẽ được coi như một phần của cảnh báo.

Hãy cùng xem một ví dụ khác. Chúng tôi có lý do để tin rằng một người trong cuộc trong tổ chức của chúng tôi đang dành thời gian tìm kiếm tài liệu tục tĩu. Mục tiêu của chúng tôi trong trường hợp này là cảnh báo cho quản trị viên về tất cả các nỗ lực sử dụng mạng bằng cổng 80 với tìm kiếm từ khóa, khiêu dâm.

Như chúng ta biết, HTTP sử dụng cổng 80. Do đó, chúng tôi sẽ tìm kiếm hoạt động mạng từ mạng của chúng tôi đến bất kỳ mạng bên ngoài nào sử dụng cổng 80 và có chứa từ khiêu dâm.

Để thực hiện việc này, hãy viết quy tắc sau:

***alert tcp $HOME\_NET any -> any 80 (content:"porn"; sid:100002;rev:2;)***

Quy tắc này sẽ đưa ra tất cả các hoạt động tìm kiếm và duyệt web với từ “porn” trong đó.

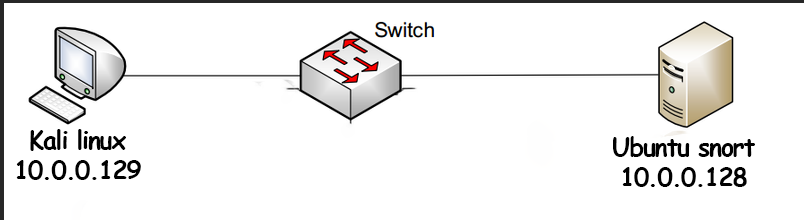
Như chúng ta có thể thấy, SNORT là một công cụ cực kỳ linh hoạt, cung cấp cho chúng ta rất nhiều khả năng để xác định cả hoạt động của người trong cuộc và người ngoài cuộc trên mạng. Tuy nhiên, để thực sự sử dụng nó hết mức, điều quan trọng là phải dành nhiều thời gian hơn cho việc luyện tập với SNORT. Toàn bộ sách đã được viết về cách sử dụng và quy tắc SNORT. Internet cũng có một số hướng dẫn tuyệt vời về việc sử dụng SNORT. Là một chuyên gia pháp y mạng tiềm năng và một Digital 007 đang thực hiện, tôi khuyên bạn nên dành thêm thời gian cho công cụ tuyệt vời này. Hướng dẫn SNORT ở dạng PDF (có trong bản phân phối) cũng là một tài nguyên tuyệt vời để nâng cao khả năng của một người dùng và sẽ là tài nguyên đầu tiên được bạn xem xét.

**KẾT LUẬN**

Trong chương này, bạn đã tìm hiểu về các hệ thống phát hiện và ngăn chặn xâm nhập mạng. Chúng ta cũng khám phá cách mỗi phương pháp có một vai trò khác nhau và cách thức khác nhau để mỗi thực hiện nhiệm vụ của riêng. Chúng ta cũng đã được tiếp xúc với SNORT, đây là một công cụ rất linh hoạt có thể được sử dụng cho cả việc bắt gói và phát hiện và ngăn chặn xâm nhập mạng. Bạn đã học được tầm quan trọng của việc tạo quy tắc cho NIDS/NIPS và khám phá cách chúng ta có thể sử dụng các quy tắc này để xác định kẻ xâm nhập trong mạng của mình. Trong chương tiếp theo, bạn sẽ tìm hiểu về một khía cạnh rất quan trọng của điều tra mạng, kết nối các liên kết bằng nhật ký mạng. Giống như một kẻ giết người để lại dấu vết bên cạn các bộ phận trên nạn nhân, một kẻ xâm nhập để lại dấu vết hoạt động của anh ta / cô ta trong nhật ký mạng. Do đó, tầm quan trọng của nhật ký mạng trong bất kỳ cuộc điều tra nào là tối quan trọng. Chương tiếp theo sẽ chuẩn bị chúng tôi từ quan điểm này.

**CHƯƠNG 3. THỰC NGHIỆM PHÁP HIỆN XÂM NHẬP MẠNG VỚI  
SNORT**

**3.1. Mô hình thử nghiệm**



*Hình 3. 1. Mô hình thử nghiệm*

Môi trường giả lập: Vmware Workstation

* Kali Linux : 10.0.0.129
* Ubuntu snort 10.0.0.128

**3.2. Cài đặt snort**

*3.2.1. Chuẩn bị*

- Bạn chuẩn bị một máy chủ cài đặt hệ điều hành Ubuntu x64. Thực hiện update hệ thống.

*apt update && apt dist-upgrade –y*

- Bắt đầu thực hiện cài đặt trước các gói mà Snort cần để chạy:

* pcap
* PCRE
* Libdnet
* DAQ

*apt install -y build-essential*

*apt install -y libpcap-dev libpcre3-dev libdumbnet-dev*

*apt install -y bison flex*

- Tạo một thư mục chứa toàn bộ source code cài đặt và cài đặt DAQ

*mkdir -p ~/snort\_src*

*cd ~/snort\_src*

*wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz*

*tar -xzvf daq-2.0.6.tar.gz*

*cd daq-2.0.6*

*./configure*

*make*

*make install*

Khi cài đặt có một số warning nhưng việc cài đặt vẫn diễn ra bình thường, ko vấn đề gì cả.

*3.2.2. Cài đặt Snort*

***-*** Cài đặt thêm một số lib cho Snort

*apt install -y zlib1g-dev liblzma-dev openssl libssl-dev libnghttp2-dev*

*-* Cài đặt snort

*cd ~/snort\_src*

*wget https://www.snort.org/downloads/snort/snort-2.9.11.1.tar.gz*

*tar -xzvf snort-2.9.11.1.tar.gz*

*cd snort-2.9.11.1*

*./configure --enable-sourcefire*

*make*

*make install*

- Chạy lệnh sau để cập nhật thư viện chia sẻ:

*ldconfig*

*-* Đưa liên kết các thư viện của Snort vào /usr/sbin

*ln -s /usr/local/bin/snort /usr/sbin/snort*

- Kiểm tra lại version của Snort sau khi cài xong

*snort –V*

*3.2.3. Cấu hình Snort chạy NIDS mode*

Sử dụng một user khác root để chạy Snort

* Tạo user và group snort

*groupadd snort*

*useradd snort -r -s /sbin/nologin -c SNORT\_IDS -g snort*

* Tạo các thư mục Snort

*mkdir /etc/snort*

*mkdir /etc/snort/rules*

*mkdir /etc/snort/rules/iplists*

*mkdir /etc/snort/preproc\_rules*

*mkdir /usr/local/lib/snort\_dynamicrules*

*mkdir /etc/snort/so\_rules*

* Tạo file để lưu trữ rule và danh sách IP

*touch /etc/snort/rules/iplists/black\_list.rules*

*touch /etc/snort/rules/iplists/white\_list.rules*

*touch /etc/snort/rules/local.rules*

*touch /etc/snort/sid-msg.map*

* Tạo thư mục lưu trữ log

*mkdir /var/log/snort*

*mkdir /var/log/snort/archived\_logs*

* Phân quyền

*chmod -R 5775 /etc/snort*

*chmod -R 5775 /var/log/snort*

*chmod -R 5775 /var/log/snort/archived\_logs*

*chmod -R 5775 /etc/snort/so\_rules*

*chmod -R 5775 /usr/local/lib/snort\_dynamicrules*

* Chuyển quyền

*chown -R snort:snort /etc/snort*

*chown -R snort:snort /var/log/snort*

*chown -R snort:snort /usr/local/lib/snort\_dynamicrules*

* Snort cần vài file cấu hình, ta sử dụng các file có sẵn trong source

*cd ~/snort\_src/snort-2.9.11.1/etc/*

*cp \*.conf\* /etc/snort*

*cp \*.map /etc/snort*

*cp \*.dtd /etc/snort*

*cd ~/snort\_src/snort-2.9.11.1/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/*

*cp \* /usr/local/lib/snort\_dynamicpreprocessor*

* Tới đây, cơ bản Snort đã được cấu hình xong, ta chỉnh lại một số thông số trong file */etc/snort/snort.conf* trước khi chạy

*sed -i "s/include \$RULE\\_PATH/#include \$RULE\\_PATH/ " /etc/snort/snort.conf*

* Sửa thủ công một số thông số khác bằng cách sử dụng lệnh *vim /etc/snort/snort.conf*

*# LINE 45 thay bằng internal network. Nếu muốn dải mạng external thì nên dùng !$HOME\_NET*

*ipvar HOME\_NET 10.0.0.0/24*

*# LINE 104*

*var RULE\_PATH /etc/snort/rules*

*var SO\_RULE\_PATH /etc/snort/so\_rules*

*var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules*

*var WHITE\_LIST\_PATH /etc/snort/rules/iplists*

*var BLACK\_LIST\_PATH /etc/snort/rules/iplists*

*# Sử dụng file local.rules thì tại dòng 546 ta bỏ dấu #*

*include $RULE\_PATH/local.rules*

* Sau khi cấu hình xong, ta verify lại file một lần bằng lệnh:

*sudo snort -T -i eth0 -c /etc/snort/snort.conf*

**3.3. Thiết lập luật cơ bản**

* Viết một rule đơn giản để test Snort Detection. ta mở file /etc/snort/rules/local.rules và thêm dòng sau

*alert icmp any any -> $HOME\_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)*

* Tiếp tục thêm dòng cấu hình sau vào rule /etc/snort/sid-msg.map để bật trigger cảnh báo

*1 || 10000001 || 001 || icmp-event || 0 || ICMP Test detected || url,tools.ietf.org/html/rfc792*

* Chạy lệnh sau để chắc chắn đã cấu hình đúng:

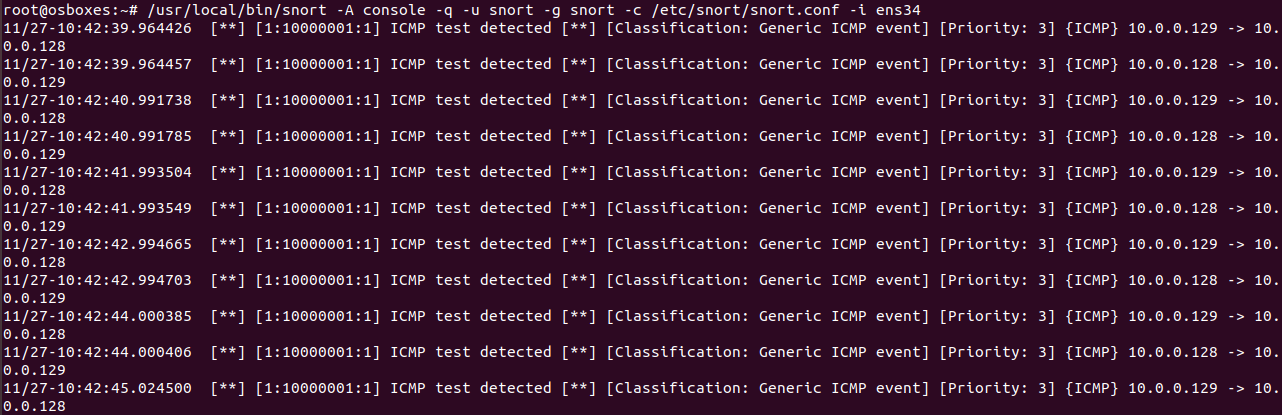
*snort -T -c /etc/snort/snort.conf -i eth0*

Một số tham số trong lệnh chạy:

* A console
* q
* u snort
* g snort
* c /etc/snort/snort.conf
* i eth0
* Thực hiện chạy lệnh sau để kiểm tra:

*/usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0*

* Đứng trên máy khác ping tới interface đang được Snort bắt gói sẽ có log tương tự sau:



*Hình 3. 2. Kết quả thực nghiệm*

* Tiến hành ping tới IP của eth0 sẽ có log alert được xuất hiện trên màn hình console. Nếu bạn ctrl-c để dừng Snort, các thông tin sẽ lưu vào trong thư mục /var/log/snort với tên snort.log.nnnnnn (số có thể khác).

# KẾT LUẬN

Qua quá trình thực hiện, nhóm nhận thấy một hệ thống mạng sẽ gặp rất nhiều vấn đề về bảo mật. Việc triển khai phần mềm Snort một phần mềm mã nguồn mở với khả năng phát hiện và ngăn chặn xâm nhập, giúp hệ thống mạng được an toàn, tăng hiệu xuất hoạt động, đảm bảo công việc và tiết kiệm chi phí. Với hệ thống phát hiện và ngăn chặn xâm nhập có thể làm cơ sở tham khảo và ứng dụng thực tế cho các nhà quản trị mạng.

Hệ thống phát hiện ngăn chặn xâm nhập mạng (NIDS/NIPS) tuy chỉ mới xuất hiện sau này nhưng hiện đóng vai trò không kém phần quan trọng. NIDS giúp con người khám phá, phân tích một nguy cơ tấn công mới. Từ đó người ta vạch ra phương án phòng chống. Ở một góc độ nào đó, có thể lần tìm được thủ phạm gây ra một cuộc tấn công. Một tổ chức lớn không thể nào thiếu NIDS/NIPS.

Tuy đã đạt được các yêu cầu đặt ra nhưng các kết quả còn khá khiêm tốn do hạn chế về tài liệu, thời gian và yêu cầu phần cứng của máy tính. Trong thời gian sắp tới, nếu có điều kiện, nhóm sẽ cố gắng phát triển thêm một số nội dung như tích hợp với các công cụ quản lý khác, lưu trữ dữ liệu log sang cơ sở dữ liệu để phục vụ quá trình phân tích được tốt hơn.

# DANH MỤC TÀI LIỆU THAM KHẢO

|  |  |
| --- | --- |
| [1] | S. Datt, "Learning Network Forensics". |
| [2] | P. Q. Tuyến, "TÌM HIỂU HỆ THỐNG PHÁT HIỆN CẢNH BÁO". |
| [3] | [Online]. Available: https://viblo.asia/p/phuong-phap-trien-khai-he-thong-phat-hien-xam-nhap-snort-aWj53pMYK6m. |
| [4] | [Online]. Available: https://upcloud.com/community/tutorials/install-snort-ubuntu/. |
| [5] | [Online]. Available: http://ipmac.vn/technology-corner/bao-mat-he-thong-voi-he-thong-idsips-phan-1. |
| [6] | [Online]. Available: https://caythongnho.wordpress.com/2018/02/09/firewall-va-ids-ips/. |