TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Báo cáo môn học

Nhập môn an toàn thông tin

Đề tài: Hệ thống phát hiện xâm nhập dựa trên bất thường

Nhóm sinh viên thực hiện:

Nguyễn Quốc Cường 20172991

Nguyễn Ngọc Trinh 20173413

Trần Trung Nghĩa 20173281

Đặng Đình Thái 20173357

Giảng viên hướng dẫn: PGS. TS Nguyễn Linh Giang

Hà Nội, tháng 6 năm 2020

Mục lục

[Lời mở đầu 3](#_Toc42256726)

[Chương 1: Tổng quan về hệ thống phát hiện xâm nhập 4](#_Toc42256727)

[1.1 Hệ thống phát hiện xâm nhập 4](#_Toc42256728)

[1.2 Kiến trúc hệ thống IDS 4](#_Toc42256729)

[1.3 Phân loại 5](#_Toc42256730)

[1.4 Các kiểu tấn công mang 7](#_Toc42256731)

[Chương 2: Hệ thống phát hiện xâm nhập dựa trên bất thường 9](#_Toc42256732)

[2.1 Thế nào là bất thường trong mạng? 9](#_Toc42256733)

[2.2 Các phương pháp phát hiện bất thường 11](#_Toc42256734)

[2.2.1 Phương pháp hệ chuyên gia 11](#_Toc42256735)

[2.2.2 Phương pháp mạng noron 12](#_Toc42256736)

[2.2.3 Phân tích thống kê 14](#_Toc42256737)

[2.2.4 Mạng Bayes 14](#_Toc42256738)

[2.2.5 Máy trạng thái hữu hạn 14](#_Toc42256739)

[Chương 3:Hệ thống phát hiện xâm nhập Snort 16](#_Toc42256740)

[3.1 Giới thiệu về Snort 16](#_Toc42256741)

[3.2 Thành phần của Snort 16](#_Toc42256742)

[3.2.1 Bộ phận giải mã gói tin (Packet Decoder) 16](#_Toc42256743)

[3.2.2 Bộ phận tiền xử lý (Reprocessors) 16](#_Toc42256744)

[3.2.3 Bộ phận phát hiện (Detection Engine) 17](#_Toc42256745)

[3.2.4 Bộ phận ghi nhận và thông báo (Loging and alerting system) 17](#_Toc42256746)

[3.2.5 Bộ phận đầu ra (Output Modules) 18](#_Toc42256747)

[3.3 Cơ chế hoạt động của Snort 18](#_Toc42256748)

[3.3.1 Sniff mode (Snort -v) 18](#_Toc42256749)

[3.3.2 Packet logger mode 18](#_Toc42256750)

[3.3.3 NIDS mode (Network Instrucsion Detection System mode) 19](#_Toc42256751)

[3.4 Cấu trúc của Rules 19](#_Toc42256752)

[3.4.1 Rule header 19](#_Toc42256753)

[3.4.2 Rule options 20](#_Toc42256754)

[Chương 4: Chương trình demo bằng Snort 23](#_Toc42256755)

[Tài liệu tham khảo 24](#_Toc42256756)

# Lời mở đầu

Ngày nay, nhu cầu trao đối dữ liệu qua hệ thống mạng máy tính trở thành vô cùng quan trọng trong mọi hoạt động của xã hội. Vấn đề bảo đảm an ninh, an toàn cho thông tin trên mạng ngày càng là mối quan tâm hàng đầu của các công ty, các tố chức, các nhà cung cấp dịch vụ. Cùng với thời gian, các kỹ thuật tấn công ngày càng tinh vi hơn khiến các hệ thống an ninh mạng trờ nên mất hiệu quả. Các hệ thống an ninh mạng truyền thống thuần túy dựa trên các tường lửa nhằm kiểm soát luồng thông tin ra vào hệ thống mạng một cách cứng nhắc dựa trên các luật bào vệ cố định. Với kiểu phòng thủ này, các hệ thống an ninh sẽ bất lực trước kỹ thuật tấn công mới, đặc biệt là các cuộc tấn công nhằm vào điếm yếu của hệ thống. Vì vậy cần phải có một hệ thống nhằm giám sát luồng thông tin vào ra trên mạng và bảo vệ các hệ thống mạng khói sự tẩn công từ Internet. Kiểm soát tài nguyên và hoạt động của hệ thống mạng, sử dụng thông tin thu thập được từ những nguồn này, thông báo cho những người có trách nhiệm khi nó xác định được khả năng có sự xâm nhập.

Hơn nữa tường lửa chỉ làm việc với những gói tin khi chúng đi vào và đi ra khỏi mạng. Một khi kẻ xâm nhập đã vượt qua được tường lửa, người đó có thể tung hoành trên mạng. Đó là lý do tại sao hệ thống phát hiện xâm nhập có vai trò quan trọng. Hệ thổng phát hiện xâm nhập IDS là hệ thống phần mềm hay phần cứng tự động thực hiện quy trình giám sát các sự kiện diễn ra trong hệ thống máy tính hay mạng máy tính, phân tích và phát hiện ra những vấn đề an ninh cho hệ thống.

Một trong những cách hoạt động của IDS là dựa trên bất thường của lưu lượng mạng. Bằng những ưu điểm vượt trội của mình, phương pháp này đang được sử dụng rộng rãi và ngày càng phát triển.

# Chương 1: Tổng quan về hệ thống phát hiện xâm nhập

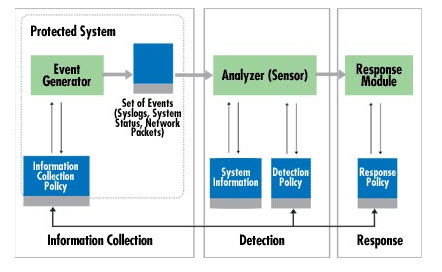
## 1.1 Hệ thống phát hiện xâm nhập

IDS là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Khác với tường lửa, IDS không thực hiện các thao tác ngăn chặn truy nhập mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng. Một điểm khác biệt khác đó là mặc dù cả hai đều liên quan đến bảo mật mạng, nhưng tường lửa theo dõi sự xâm nhập từ bên ngoài và ngăn chặn chúng xảy ra, nó giới hạn truy nhập giữa các mạng để ngăn chặn sự xâm nhập nhưng không phát hiện được cuộc tấn công từ bên trong mạng. Bên cạnh đó IDS sẽ đánh giá sự xâm nhập đáng ngờ khi nó đã diễn ra đồng thời phát ra cảnh báo, nó theo dõi được các cuộc tấn công có nguồn gốc từ bên trong một hệ thống. Chức năng ban đầu của IDS chỉ là phát hiện các dấu hiện xâm nhập, do đó IDS chỉ có thể tạo ra các cảnh báo tấn công khi tấn công đang diễn ra hoặc thậm chí sau khi tấn công đã hoàn tất. Càng về sau, nhiều kỹ thuật mới được tích hợp vào IDS, giúp nó có khả năng dự đoán được tấn công (prediction) và thậm chí phản ứng chủ động các tấn công đang diễn ra (Active response).

## 1.2 Kiến trúc hệ thống IDS

Kiến trúc của hệ thống IDS bao gồm 3 thành phần chính: Thành phần thu thập gói tin (information collection), thành phần phân tích gói tin ( Dectection), thành phần phản hồi (respontion) nếu gói tin đó được phát hiện là một tấn công của tin tặc. Trong 3 thành phần này thì thành phần phân tích gói tin là một thành phần quan trọng nhất và ở thành phần này bộ cảm biến đóng vai trò quyết định nên chúng ta đi sâu vào phân tích bộ cảm biến để hiểu rõ hơn kiến trúc của hệ thống phát hiện xâm nhập là như thế nào.

Bộ cảm biến được tích hợp với thành phần sưu tập dữ liệu – một bộ tạo sự kiện. Cách sưu tập này được xác định bởi chính sách tạo sự kiện để định nghĩa chế độ lọc thông tin sự kiện. Bộ tạo sự kiện (hệ điều hành, mạng, ứng dụng) cung cấp một số chính sách thích hợp cho các sự kiện, có thể là một bản ghi các sự kiện của hệ thống hoặc các gói mạng. Số chính sách này cùng với thông tin chính sách có thể được lưu trong hệ thống được bảo vệ hoặc bên ngoài. Trong trường hợp nào đó, ví dụ khi luồng dữ liệu sự kiện được truyền tải trực tiếp đến bộ phân tích mà không có sự lưu dữ liệu nào được thực hiện. Điều này cũng liên quan một chút nào đó đến các gói mạng.



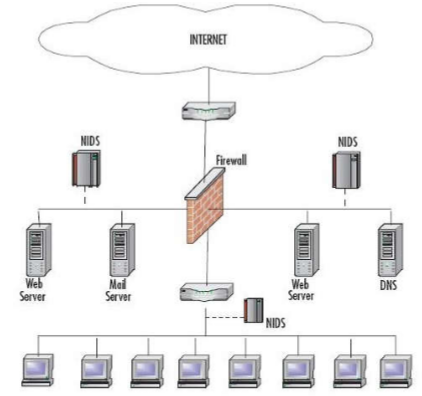
Kiến trúc hệ thống IDS

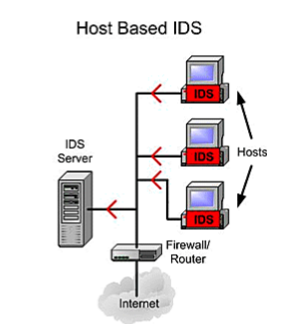
Vai trò của bộ cảm biến là dùng để lọc thông tin và loại bỏ dữ liệu không tương thích đạt được từ các sự kiện liên quan với hệ thống bảo vệ, vì vậy có thể phát hiện được các hành động nghi ngờ. Bộ phân tích sử dụng cơ sở dữ liệu chính sách phát hiện cho mục này. Ngoài ra còn có các thành phần: dấu hiệu tấn công, profile hành vi thông thường, các tham số cần thiết (ví dụ: các ngưỡng). Thêm vào đó, cơ sở dữ liệu giữa các tham số cấu hình, gồm có các chế độ truyền thông với module đáp trả. Bộ cảm biến cũng có cơ sở dữ liệu của riêng nó, gồm dữ liệu lưu về các xâm phạm phức tạp tiềm ẩn (tạo ra từ nhiều hành động khác nhau).

IDS có thể được sắp đặt tập trung (ví dụ như được tích hợp vào trong tường lửa) hoặc phân tán. Một IDS phân tán gồm nhiều IDS khác nhau trên một mạng lớn, tất cả chúng truyền thông với nhau. Nhiều hệ thống tinh vi đi theo nguyên lý cấu trúc một tác nhân, nơi các module nhỏ được tổ chức trên một host trong mạng được bảo vệ.

## 1.3 Phân loại

* Dựa trên phạm vi giám sát, IDS được chia thành 2 loại:
  + Network-based IDS (NIDS): Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau tường lửa.



* + Host-based IDS (HIDS): Là những IDS giám sát hoạt động của từng máy tính riêng biệt. Do vậy, nguồn thông tin chủ yếu của HIDS ngòai lưu lượng dữ liệu đến và đi từ máy chủ còn có hệ thống dữ liệu nhật ký hệ thống (system log) và kiểm tra hệ thống (system audit).  
    
* Dựa trên kỹ thuật phát hiện, IDS cũng được chia thành 2 loại:
  + Signature-based IDS: Signature-based IDS phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập, thông qua phân tích lưu lượng mạng và log 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.
  + Anomaly-based IDS: phát hiện xâm nhập bằng cách so sánh (mang tính thống kê) 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. Ví dụ, trong điều kiện bình thường, lưu lượng trên một giao tiếp mạng của server là vào khỏang 25% băng thông cực đại của giao tiếp. Nếu tại một thời điểm nào đó, lưu lượng này đột ngột tăng lên đến 50% hoặc hơn nữa, thì có thể giả định rằng server đang bị tấn công DoS. Để hoạt động chính xác, các IDS loại này phải thực hiện một quá trình “học”, tức là giám sát hoạt động của hệ thống trong điều kiện bình thường để ghi nhận các thông số hoạt động, đây là cơ sở để phát hiện các bất thường về sau.

## 1.4 Các kiểu tấn công mang

Trong lịch sử tồn tại của mạng máy tính đã từng xảy ra rất nhiều các cuộc tấn công mạng với qui mô lớn, nhỏ khác nhau và cũng để lại nhiều thiệt hại nghiêm trọng. Có nhiều cách thức tấn công nhưng chúng ta có thể phân thành bốn loại hình tấn công mạng chính như sau:

* DoS- Denial of Service attack : Là những tấn công làm cho tài nguyên máy tính (ví dụ Web server) không phục vụ được theo yêu cầu của người dùng thực sự . Dạng phổ biến nhất của tấn DoS là làm cho tài nguyên máy tính quá bận vì bị sử dụng toàn bộ với rất nhiều yêu cầu vô ích đến mức người dùng thực sự không thể sử dụng nó. Có rất nhiều biến thể của tấn công DoS bao gồm TCP-SYN Flood, ICMP/UDP Flood, Smurf, Ping of Death, Teardrop, Mailbomb, Apache2...
* R2L - Remote to Local attack : Trong loại tấn công này, tin tặc cố gắng đạt được quyền truy cập vào khu vực hệ thống máy tính bằng việc gửi các gói tin tới hệ thống thông qua mạng. Một vài cách phổ biến mà loại này thực hiện là đoán mật khẩu thông qua phương pháp từ điển brute-force, FTP Write,...
* U2R - User to Root attack : Trong kiểu tấn công này, tin tặc với quyền của một người dùng bình thường cố gắng để đạt được quyền truy nhập cao nhất (đặc quyền của người quản trị) vào hệ thống một cách bất hợp pháp. Cách thức phổ biến của kiểu tấn công này là gây tràn bộ đệm.
* Probe - Surveillance : Trong loại tấn công này, tin tặc quét mạng hoặc máy tính để tìm ra điểm yếu dễ tấn công mà thông qua đó tin tặc có thể khai thác hệ thống. Điều này có phần giống như theo dõi, giám sát hệ thống. Một cách phổ biến của loại tấn công này là thực hiện thông qua việc quét các cổng của hệ thống máy tính. Bằng việc này, tin tặc có thể lấy được thông tin về cổng đang mở, dịch vụ đang chạy, và rất nhiều thông tin chi tiết nhạy cảm khác như địa chỉ IP, địa chỉ MAC, các luật tường lửa đang sử dụng,...

# Chương 2: Hệ thống phát hiện xâm nhập dựa trên bất thường

## 2.1 Thế nào là bất thường trong mạng?

Sự bất thường trong mạng thường dùng để chỉ những tình huống khi hoạt động của mạng đi chệch so với các trạng thái được quy định là bình thường. Bất thường trong mạng có thể phát sinh từ nhiều nguyên nhân như các thiết bị mạng bị hỏng hóc, hệ thống mạng quá tải, hệ thống gặp phải các cuộc tấn công từ chối dịch vụ, hoặc các cuộc xâm nhập phá vỡ khả năng vận chuyển của các dịch vụ mạng .... Những sự kiện bất thường sẽ phá vỡ trạng thái bình thường của một vài dữ liệu mạng mà chúng ta có thể đo được. Người ta sẽ dựa vào trạng thái của các dữ liệu này để xác định trạng thái của mạng là bình thường hay không bình thường. Các dữ liệu dùng để xác định trạng thái của mạng phụ thuộc vào một vài nhân tố đặc biệt như khả năng hoạt động của một hệ thống dựa trên dung lượng lưu thông, loại dữ liệu hệ thống sẵn có, những ứng dụng đang chạy trên hệ thống, các gói tin gửi đến với những yêu cầu hệ thống thực hiện những câu lệnh nhạy cảm...

Như vây, những bất thường của hệ thống được xác định thông qua những thay đổi nhanh liên tục trong dữ liệu hệ thống trước hoặc trong khi một sự kiện bất thường đang xảy ra. Những thay đổi nhanh dùng để diễn tả sự thay đổi đột ngột trong dữ liệu xảy ra theo một trật tự thời gian (tần suất). Khoảng thời gian diễn ra các thay đổi đột ngột này biến thiên theo bản chất của sự kiện bất thường đó.

Bất thường trong mạng có thể được chia làm hai lớp chính:

- Lớp bất thường thứ nhất: liên quan đến những sự cố và những lỗi về hiệu năng của mạng như sự cố liên quan đến File Server, sự cố phân trang bộ nhớ qua mạng (paging across the network), broadcast storms, babbling node, hay tắc nghẽn đường truyền (transient congestion). Ví dụ cho sự cố File Server đó là sự cố của một Web Server, xảy ra khi có một số lượng lớn yêu cầu tới máy chủ vượt quá khả năng đáp ứng. Sự cố phân trang qua mạng (paging network) xảy ra khi một chương trình ứng dụng phình to hơn dung lượng bộ nhớ giới hạn của máy trạm làm việc và bắt đầu phân trang bộ nhớ tới một File Server, việc này không ảnh hưởng đến cá nhân người dùng nhưng nó ảnh hưởng đến những người dùng khác do sẽ gây ra sự thiếu hụt băng thông mạng. Vấn đề babbling node là tình huống khi một nốt mạng gửi ra ngoài những gói tin nhỏ trong một vòng lặp vô hạn để kiểm tra một vài thông tin như các báo cáo về trạng thái... Trong một vài trường hợp những lỗi phần mềm cũng có thể gây ra các bất thường trong mạng như những lỗi khi xây dựng giao thức mạng khiến cho một máy liên tục gửi các gói tin gây tắc nghẽn mạng...

- Lớp bất thường thứ 2: là những vấn đề liên quan đến an ninh mạng. Ví dụ về những bất thường dạng này là tấn công từ chối dịch vụ (DoS). Tấn công từ chối dịch vụ là một trong những thủ đoạn nhằm ngăn cản những người dùng hợp pháp khả năng truy cập và sử dụng vào một dịch vụ nào đó. DoS có thể làm ngưng hoạt động của một máy tính, một mạng nội bộ thậm chí cả một hệ thống mạng rất lớn. Về bản chất thực sự của DoS, kẻ tấn công sẽ chiếm dụng một lượng lớn tài nguyên mạng như băng thông, bộ nhớ... và làm mất khả năng xử lý các yêu cầu dịch vụ từ các khách hàng khác. Tấn công DoS nói chung không nguy hiểm như các kiểu tấn công khác, vì kẻ tấn công ít có khả năng thâm nhập hay chiếm được thông tin dữ liệu của hệ thống. Tuy nhiên, nếu máy chủ tồn tại mà không thể cung cấp thông tin, dịch vụ cho người sử dụng thì sự tồn tại này là không có ý nghĩa, đặc biệt là các hệ thống phục vụ các giao dịch điện tử thì thiệt hại là vô cùng lớn. Đối với hệ thống máy chủ được bảo mật tốt, khó thâm nhập, việc tấn công từ chối dịch vụ DoS được các hacker sử dụng như là “quân cờ cuối” để triệt hạ hệ thống đó.

## 2.2 Các phương pháp phát hiện bất thường

### 2.2.1 Phương pháp hệ chuyên gia

Phương pháp này ra đời từ rất sớm và được ứng dụng vào lĩnh vực dò lỗi hay phát hiện bất thường trong mạng. Trong hệ chuyên gia, một cơ sở dữ liệu chứa tập luật (rules) miêu tả các hành vi bất thường được dùng để so sánh với các luồng dữ liệu đi đến hệ thống mạng. Nếu một luồng dữ liệu đi đến hệ thống với mục đích tấn công mà không được định nghĩa trong tập luật thì hệ thống IDS không thể phát hiện được.Trên thực tế phương pháp này được áp dụng cho hệ thống phát hiện xâm nhập Snort rất nổi tiếng. Snort là hệ thống IDS mã nguồn mở, được cung cấp miễn phí hầu hết các tập luật, nhưng nếu chúng ta muốn sử dụng các tập luật mới hơn, đầy đủ hơn thì có thể mua thêm gói rules mất phí.

Hệ thống phát hiện bất thường dựa trên rule-based có đặc điểm dễ cấu hình, dễ thêm luật mới và dễ sử dụng. Mỗi khi hệ thống mạng đứng trước những nguy cơ tấn công mới, người quản trị chỉ việc cập nhật thêm các luật chưa có vào cơ sở dữ liệu. Phương pháp này có tỉ lệ phát hiện nhầm rất thấp vì nó dùng cách phân tích gói tin và so sánh với mẫu đã có.

Tuy nhiên hệ thống phát hiện xâm nhập dựa trên rule-based sẽ trở nên chậm chạp dần khi tập luật phình to lên. Khi khối lượng luật quá lớn hệ thống sẽ không đáp ứng được yêu cầu của các ứng dụng thời gian thực. Những bất cập xảy ra có thể là: gói tin bị nghẽn cổ chai, số lượng kết nối TCP mở nhiều trên mức cho phép, băng thông đạt mức tối đa ... Phương pháp này còn có một nhược điểm là phụ thuộc khá nhiều vào người quản trị mạng và không đáp ứng kịp khi hệ thống mạng được mở rộng do mỗi khi hệ thống có sự thay đổi thì cần có sự bổ sung về tập luật. Người ta có thể sử dụng mô hình hệ chuyên gia FCMs (fuzzy cognitive maps) để khắc phục nhược điểm này. FCMs có thể được sử dụng để tạo ra một mô hình thông minh có sự thừa kế và tác động qua lại với nhau giữa các triệu chứng mạng. Cơ chế hoạt động của phương pháp rule-based có thể diễn giải như sau:

- Giả thiết các sự kiện phát triển theo một trình tự nhất định.

- Mô tả hành vi hoạt động bình thường của hệ thống dưới dạng các luật đã được rút gọn nhất có thể. Ví dụ như A1 -> A2 -> B1, sự kiện A1 xảy ra xong đến sự kiện A2 thì có thể xảy ra sự kiện B1 tiếp theo.

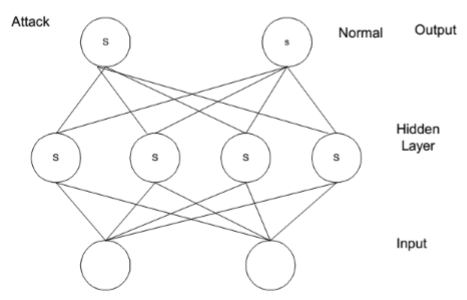
- Ta có một tập luật, so sánh các chuỗi sự kiện đưa vào với tập luật, nếu các sự kiện đưa vào phù hợp với vế trái của một luật mà không trùng với về phải của luật đó thì có thể xem xét xác định bất thường ở đây. Như ở ví dụ trên trong thực tế sự kiện Al dẫn đến sự kiện A2, nhưng sự kiện A2 xảy ra cuối cùng lại dẫn đến sự kiện C1 mà không phải là B1 thì có thể kết luận là có sự kiện bất thường diễn ra ở đây.

### 2.2.2 Phương pháp mạng noron

Như chúng ta đã nghiên cứu ở trên, một trong những phương pháp phổ biến dùng để phát hiện bất thường là hệ chuyên gia, tuy nhiên phương pháp này có nhược điểm là phụ thuộc khá nhiều vào tập luật được định nghĩa trước bởi người quản trị và phải được cập nhật thường xuyên. Nhược điểm này có thể được khắc phục bằng cách áp dụng công nghệ mạng nơ-ron. Phương pháp này ra đời với mục đích khắc phục việc phải cập nhật các luật mới có thể tạo ra xung đột trong tập luật đã có, vốn chỉ phù hợp với các mô hình quy mô vừa và nhỏ. Thay vào đó hệ thống IDS sẽ được học mô hình phát hiện bất thường dựa trên một số lượng nhất định các mẫu dữ liệu được thu thập. Hiệu quả của phương pháp này thường cho ra hệ thống có khả năng tốt hơn đồng thời lại linh động trong thay đổi huấn luyện. Với cách tiếp cận này, người ta có thể dễ dàng hơn trong việc xây dựng các hệ thống IDS phức tạp, việc phát hiện xâm nhập không đơn thuần chỉ là phát hiện nhằm cảnh báo có tấn công hay không tấn công mà còn có thể đưa ra loại hình, tính chất chi tiết của cuộc tấn công tương ứng.

Hệ thống phân tích bất thường sử dụng mạng nơ-ron tập trung vào việc phát hiện các thay đổi trong hành vi, theo đó mạng nơ-ron sẽ học và dự đoán hành vi của người sử dụng, của các chương trình ứng dụng và các luồng tin từ bên ngoài đi vào mạng. Ưu điểm của mạng nơ-ron là thích ứng được với các kiểu dữ liệu không đầy đủ, dữ liệu với độ chắc chắn không cao và không cần cập nhật tri thức thường xuyên do nó có quá trình tự học.

Mạng nơ-ron nhân tạo hay thường gọi ngắn gọn là mạng nơ-ron là một mô hình tính toán được xây dựng dựa trên cấu tạo của mạng nơ-ron sinh học. Nó gồm có một nhóm các nơ-ron nhân tạo (nút) nối với nhau, và xử lý thông tin bằng cách truyền theo các kết nối và tính giá trị mới tại các nút. Trong nhiều trường hợp, mạng nơ-ron nhân tạo là một hệ thống thích ứng (adaptive system) tự thay đổi cấu trúc của mình dựa trên các thông tin bên ngoài hay bên trong đi qua mạng trong quá trình học



Một mạng nơ-ron bao gồm các nút input (đầu vào), các nút trong các lớp ẩn (hidden layer) và nút output,cấu trúc mạng nơ-ron được chia thành 2 loại:

Loại thứ nhất sử dụng các thuật toán huấn luyện được giám sát (Supervised training algorithms), ở giai đoạn tự học, hệ thống có khả năng tính toán một đầu ra mong muốn cho mỗi đầu vào đã được định sẵn. Cấu trúc phổ biến của mạng nơ-ronhọc có giám sát là kiến trúc nhận thức đa tầng MLP(Multi-layerPerceptron). MLP là mạng chuyển tiếp đa tầng (feed-forward) bao gồm lớp đầu vào, một hoặc một vài lớp ẩn và lớp đầu ra. Lớp đầu ra cung cấp phản hồi của hệ thống đến các mẫu hoạt động trong lớp đầu vào. Nghiên cứu MLP nhằm giải quyết dạng bài toán phân lớp trạng thái hệ thống, nghĩa là tìm cách phân loại trạng thái hệ thống mạng là bình thường hay bị tấn côngDoS, hay Probe (bị thăm dò)...và có thể mở rộng thêm nhiều lớp trạng thái hơn như U2R (chiếm quyền root thông qua quyền user), R2L (remote to local). Mục đích của MLP là dựa trên các mẫu đầu vào được gán nhãn để học tập, sau khi học xong nó có khả năng phân loại các mẫu đầu vào chưa có nhãn vào một trong các lớp như: bình thường, DoS hoặc Probe...Sự phân lớp được thể hiện theo cách sau: số 1 ở cột nào thì biểu thị sự xuất hiện/tồn tại dấu hiệu tương ứng của cột đó, còn số 0 biểu thị sự không tồn tại. Vì vậy chúng ta có 3 trường hợp có thể nhận biết được kết quả ở đầu ra, đó là: [1 0 0] - tình trạng bình thường, [0 1 0] cho tấn công dạng DoSvà [0 0 1] nếu gặp tấn công dạng Probe.

Loại thứ hai sử dụng các thuật toán đào tạo không giám sát (Unsupervised training algorithms): ở giai đoạn tự học, hệ thống sẽ nghiên cứu mà không xác định đầu ra mong muốn. Các bản đồ tổ chức độc lập (SOM - Self-Organizing Maps) là một dạng tiêu biểu của loại này. Trong hệ thống phát hiện bất thường sử dụng SOM, người ta tập trung vào việc phân lớp các hành vi từ đó phát hiện ra các hành vi nghi vấn. Tiến trình xử lý của hệ thống diễn ra như sau: các dữ liệu về mạng được thể hiện dưới dạng vectơ tham số đặc trưng, sau đó được lưu trong một Input vectơ để tiến hành phân lớp, việc phân lớp sẽ lặp đi lặp lại cho đến khi hội tụ, khi đã xây dựng được các SOM, hệ thống sẽ tiến hành xác định khoảng cách giữa hành vi đang xét với hành vi bình thường, nếu nó vượt quá ngưỡng cho phép thì có bất thường xảy ra ở đây.

### 2.2.3 Phân tích thống kê

Sử dụng thống kê để xác định các sự kiện bất thường được áp dụng rộng rãi trong các hệ thống phát hiện truy nhập từ nhiều thập kỷ nay. Hệ thống hoạt động trên nguyên tắc thu thập dữ liệu của các thông số trên mạng và áp dụng một số kỹ thuật thống kê trên dữ liệu thu thập được để tạo ra các tập hồ sơ cho các thông số trong thời điểm hoạt động bình thường. Ví dụ hệ thống có thể nghiên cứu sự phân phối của các thông số được giám sát, sau đó nó sẽ xem xét sự khác nhau giữa thông số ở thời điểm hiện tại với tệp hồ sơ đã lập, thông thường nếu dữ liệu của thông số hiện tại cao hơn thì nhiều khả năng hệ thống bị tấn công. Hệ thống có thể sử dụng nhiều quy luật đơn giản để phát hiện ra sự khác nhau. Sử dụng ngưỡng (threshold) là cách đơn giản nhất, khi thông số được theo dõi vượt quá ngưỡng đặt ra thì có cảnh báo. Các hệ thống sử dụng phân tích thống kê điển hình là Haystack (Smaha, 1988), IDES (Lunt et al, 1988), EMERALD(Porras and Neumann, 1997).

### 2.2.4 Mạng Bayes

Mạng Bayes là mô hình đồ thị thể hiện mối quan hệ nguyên nhân - kết quả, dựa chủ yếu trên lý thuyết xác suất có điều kiện kết hợp với lý thuyết đồ thị để giải quyết hai vấn đề quan trọng là tính không chắc chắn và tính phức tạp, do đó được ứng dụng rộng rãi.

Mạng Bayes hoạt động trên nguyên tắc mô tả mối quan hệ phụ thuộc giữa các biến, nó có thể hoạt động được trong trường hợp dữ liệu không đầy đủ và phân bố không đều như dữ liệu mạng. Ưu điểm của mạng Bayes là tính ổn định với dữ liệu đồng thời nó có khả năng đoán trước được kết quả của một hành vi do sử dụng mối quan hệ nhân quả. Các hệ thống phát hiện bất thường dựa trên mạng Bayes là mô hình của Valdes, có khả năng phát hiện các chuỗi tấn công phân tán trong khi từng tấn công tách biệt không sinh ra cảnh báo. Mô hình này sử dụng hệ thống Bayes để xây dựng mối quan hệ nguyên nhân kết quả giữa tấn công và các yếu tố quan sát. Sau đó dựa trên phân bố xác suất của các yếu tố quan sát được để tính xác suất có tấn công. Một mô hình khác là của Kruegel sử dụng cách tiếp cận là sử dụng nhiều bộ cảm ứng khác nhau, đầu ra của các bộ cảm ứng này đuợc tập hợp để sinh ra cảnh báo. Các bộ cảm ứng sẽ sử dụng phươmg pháp Bayes.

Việc sử dụng mạng Bayes cho phát hiện bất thường có ưu điểm là giảm được tỷ lệ cảnh báo sai. Tuy nhiên nó có hạn chế là hiệu suất hoạt động giảm khi các yếu tố quan sát tăng lên.

### 2.2.5 Máy trạng thái hữu hạn

Mô hình máy trạng thái hữu hạn (FSM - finite States machine) phát hiện bất thường bằng cách mô hình hóa các trạng thái hoạt động bình thường của mạng, sau đó cho dữ liệu đi qua là chuỗi các hành vi cần kiểm tra bất thường, bất thường có thể xác định nếu chuỗi đi qua không đạt được trạng thái kết thúc. Mô hình FSM xây dựng dựa trên cơ sở đặt các chuỗi báo động (sequence of alarm) ở các điểm khác nhau trên mạng để ghi lại trạng thái của máy. Theo cách thông thường một máy trạng thái hữu hạn được định nghĩa bởi một tập Q = (Q,∑, q0, phi, F) với:

- Q : tập các trạng thái có thể

- q0: trạng thái ban đầu

- ∑: tập ngôn ngữ hữu hạn

- phi : là hàm chuyển Q x ∑ -> Q

- F là tập con của Q: tập các trạng thái kết thúc

Người ta thường dùng máy trạng thái hữu hạn để xác định bất thường trong các giao thức, các giao thức này sẽ được theo dõi một cách độc lập và coi như không bị ảnh hưởng bởi các sự kiện khác. Ví dụ với giao thức TCP chúng ta có mô hình kiểm tra.

Phương pháp phát hiện bất thường sử dụng máy trạng thái hữu hạn có ưu điểm là chúng ta có thể xác định chính xác nguyên nhân gây ra bất thường, phân biệt được đó có phải là một cuộc tấn công hay không vì xây dựng được mô hình hoạt động của các sự kiện. Nhưng trên thực tế phương pháp này rất khó triển khai do rất tốn tài nguyên, phải có một tập dữ liệu lớn đầy đủ về hoạt động của mạng, có máy hiệu năng lớn để tính toán. Các sự kiện khác nhau phải xây dựng các mô hình riêng, độc lập để theo dõi.

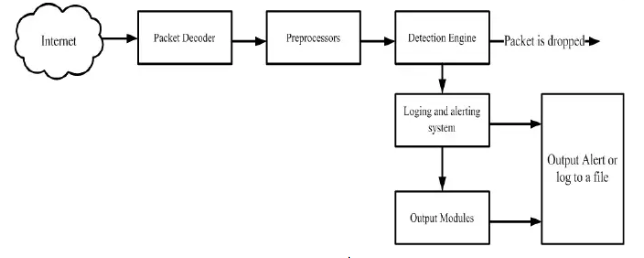
# Chương 3:Hệ thống phát hiện xâm nhập Snort

## 3.1 Giới thiệu về Snort

Snort là phần mềm IDS được phát triển bởi Martin Roesh dưới dạng mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Tuy snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời. Với kiến trúc kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình. Snort có thể chạy trên nhiều hệ thống như Windows, Linux, OpenBSD, FreeBSD, Solaris …

Bên cạnh việc có thể hoạt động như một ứng dụng bắt gói tin thông thường, Snort còn được cấu hình để chạy như một NIDS.

## 3.2 Thành phần của Snort



### 3.2.1 Bộ phận 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 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. Có thể kích hoạt hoặc vô hiệu hóa các cảnh báo dài dòng cho tất cả các trường trong tập tin snort.conf.

Sau khi dữ liệu được giải mã đúng, chúng sẽ được gửi đến bộ phận tiền xử lý (preprocessor).

### 3.2.2 Bộ phận tiền xử lý (Reprocessors)

Bộ phận tiền xử lý là một thành phần rất quan trọng đối với bất kỳ một hệ thống IDS nào để có thể chuẩn bị gói dữ liệu đưa vào cho mudule phát hiện phân tích. Ba nhiệm vụ chính của các module loại này là:

* Kết hợp lại các gói tin: Khi một dữ liệu lớn được gửi đi, thông tin sẽ không đóng gói toàn bộ vào một gói tin mà thực hiện phân mảnh, chia thành nhiều gói tin rồi mới gửi đi. Khi Snort nhận được các gói tin này, nó phải thực hiện kết nối lại để có gói tin ban đầu. Module tiền xử lý giúp Snort có thể hiểu được các phiên làm việc khác nhau.
* Giải mã và chuẩn hóa giao thức (decode/normalize): công việc phát hiện xâm nhập dựa trên dấu hiệu nhận dạng nhiều khi thất bại khi kiểm tra các giao thức có dữ liệu có thể được biểu diễn dưới nhiều dạng khác nhau. Ví dụ: một Web server có thể nhận nhiều dạng URL: URL viết dưới dạng hexa/unicode hay URL chấp nhận dấu / hay \. Nếu Snort chỉ thực hiện đơn thuần việc so sánh dữ liệu với dấu hiệu nhận dạng sẽ xảy ra tình trạng bỏ sót hành vi xâm nhập. Do vậy, 1 số Module tiền xử lý của Snort phải có nhiệm vụ giải mã và chỉnh sửa, sắp xếp lại các thông tin đầu vào.
* Phát hiện các xâm nhập bất thường (nonrule/anormal): các plugin dạng này thường để xử lý với các xâm nhập không thể hoặc rất khó phát hiện bằng các luật thông thường. Phiển bản hiện tại của Snort có đi kèm 2 plugin giúp phát hiện xâm nhập bất thường đó là portscan và bo (backoffice). Portscan dùng để đưa ra cảnh báo khi kẻ tấn công thực hiện quét cổng để tìm lỗ hổng. Bo dùng để đưa ra cảnh báo khi hệ thống nhiễm trojan backoffice.

### 3.2.3 Bộ phận phát hiện (Detection Engine)

Đây là module quan trọng nhất của Snort. Nó chịu trách nhiệm phát hiện các dấu hiệu xâm nhập. Module phát hiện sử dụng các luật được định nghĩa trước để so sánh với dữ liệu thu thập được, từ đó xác định xem có xâm nhập xảy ra hay không.

Một vấn đề quan trọng đối với module phát hiện và vấn đề thời gian xử lý gói tin: một IDS thường nhận rất nhiều gói tin và bản thân nó cũng có rất nhiều luật xử lý. Khi lưu lượng mạng quá lớn có thể xảy ra việc bỏ sót hoặc không phản hồi đúng lúc. Khả năng xử lý của module phát hiện phụ thuộc vào nhiều yếu tố: số lượng các luật, tốc độ hệ thống, băng thông mạng.

Một module phát hiện có khả năng tách các phần của gói tin ra và áp dụng luật lên từng phần của gói tin:

* IP header
* Header ở tầng transport: TCP, UDP
* Header ở tầng application: DNS, HTTP, FTP …
* Phần tải của gói tin

Do các luật trong Snort được đánh số thứ tự ưu tiên nên 1 gói tin khi bị phát hiện bởi nhiều luật khác nhau, cảnh báo được đưa ra theo luật có mức ưu tiên cao nhất.

### 3.2.4 Bộ phận ghi nhận và thông báo (Loging and alerting system)

Tùy thuộc vào module phát hiện có nhận dạng được xâm nhập hay không mà gói tin có thể bị ghi log hay đưa ra cảnh báo. Các file log là các file dữ liệu có thể ghi dưới nhiều định dạng khác nhau như tcpdump

### 3.2.5 Bộ phận đầu ra (Output Modules)

Module này thực hiện các thao tác khác nhau tùy thuộc vào việc cấu hình lưu kết quả xuất ra như thế nào.

* Ghi log file
* Ghi syslog
* Ghi cảnh báo vào cơ sở dữ liệu
* Tạo file log XML
* Cấu hình lại Router, firewall
* Gửi các cảnh báo được gói trong gói tin sử dụng giao thức SNMP

## 3.3 Cơ chế hoạt động của Snort

### 3.3.1 Sniff mode (Snort -v)

Ở chế độ này, Snort hoạt động như một chương trình thu thập và phân tích gói tin thông thường. Không cần sử dụng file cấu hình, các thông tin Snort sẽ thu được khi hoạt động ở chế độ này:

* Ngày và giờ thu thập gói tin (Date and time)
* Địa chỉ IP nguồn (Source IP address)
* Cổng nguồn (Source port number)
* Địa chỉ IP đích (Destination IP address)
* Cổng đích (Destination port number)
* Giao thức ở tầng giao vận được dùng trong gói tin (Transport layer protocol usedin this packet)
* Thời gian hoạt động của gói tin trên mạng (Time to live or TTL value in this packet)
* Thông số gói tin (Packet ID)
* Độ dài phần tiêu đề của IP (Length of IP header)
* Dữ liệu (IP payload)

Để có thể chạy ở chế độ này, chúng ta sử dụng câu lệnh: Snort -v

Ngoài ta còn kết hợp với một số thông số để hiển thị được nhiều thông tin hơn:

-v đưa ra packet headers trong phần output

-d hiển thị packet payload

-a hiển thị ARP packets

-e hiển thị dữ liệu lớp data link

### 3.3.2 Packet logger mode

Khi chạy ở chế độ này, Snort sẽ tập hợp tất cả các packet nó thấy được và đưa vào log theo cấu trúc phân tầng. Một thư mục mới sẽ được tạo ra ứng với mỗi địa chỉ nó bắt được, và dữ liệu sẽ phụ thuộc vào địa chỉ mà nó lưu trong thư mục đó. Snort đặt các packet vào trong file ASCII, với tên liên quan đến giao thức và cổng. Sự sắp xếp này dễ dàng nhận ra ai đang kết nối vào mạng của mình và giao thức, cổng nào đang sử dụng. Đơn giản sử dụng ls-R để hiện danh sách các thư mục. Tuy nhiên sự phân cấp này sẽ tạo ra nhiều thư mục trong giờ cao điểm nên rất khó để xem hết tất cả thư mục và file này. Nếu ai đó sử dụng full scan với 65536 TCP Port và 65535 UDP ports và sẽ tạo ra 131000 hoặc từng ấy file . Log với dạng nhị phân (binary) tất cả những gì có thể đọc được bởi Snort, nó làm tăng đốc độ khả năng bắt gói tin của Snort. Hầu hết các hệ thống có thể capture và log ở tốc độ 100Mbps mà không có vấn đề gì.

### 3.3.3 NIDS mode (Network Instrucsion Detection System mode)

Snort thường được sử dụng như một NIDS. Nó nhẹ, nhanh chóng, hiệu quả và sử dụng các rule để áp dụng lên gói tin. Khi phát hiện có dấu hiệu tấn công ở trong gói tin thì nó sẽ ghi lại và tạo thông báo. Khi dùng ở chế độ này phải khai báo file cấu hình cho Snort hoạt động. Thông tin về thông báo khi hoạt động ở chế độ này:

- Fast mode: Ghi lại cảnh báo trong một định dạng đơn giản với các thông tin Date and time, Alert message, Source and destination IP address, Source and destination ports, Type of packet.

- Full mode: Đây là chế độ cảnh báo mặc định và sẽ được sử dụng tự động nếu chúng ta không thay đổi cấu hình. Gồm các thông tin như chế độ fast mode và thêm một số thông tin nsau: TTL value, TOS value, Length of packet header, length of packet, Code of packet, ID of packet, Sequence number.

- Unsock mode: Gửi cảnh báo đến một UNIX socket là một chương trình khác, có thể lắng nghe trên đó.

- None mode: Tắt chế độ cảnh báo

- Console mode: Gửi tiêu đề của cảnh báo bằng dòng lệnh ra màn hình.

## 3.4 Cấu trúc của Rules

Tìm hiểu một ví dụ:

*alert tcp 192.168.0.0/22 23 -> any any (content:”confidential”; msg: “Detected confidential”)*

Ta thấy cấu trúc có dạng sau:

RULE HEADER (RULE OPTION)

* Phần Header: chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa tiểu chuẩn để áp dụng luật với gói tin đó.
* Phần Option: chứa thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh với gói tin.

### 3.4.1 Rule header

Cấu trúc của phần header: Action| Protocol| Address | Port| Direction| Address| Port

Trong ví dụ trên: Alert | TCP | 192.168.0.0/22| 23 | -> | Any | Any

* Action: là phần quy định loại hành động nào được thực thi. Thông thường các hành động rạo ra một cảnh báo hoặc log thông điệp hay kích hoạt một luật khác.  
  Có 5 luật được định nghĩa:   
  + Pass: cho phép Snort bỏ qua gói tin này  
  + Log: dùng để log gói tin. Có thể log vào file hay vào CSDL  
  + Alert: gửi thông điệp cảnh báo khi dấu hiệu xâm nhập được phát hiện  
  + Activate: tạo ra cảnh báo và kích hoạt thêm các luật khác để kiểm tra thêm điều kiện của gói tin  
  + Dynamic: đây là luật được gọi bởi các luật khác có hành động là Activate
* Protocol: giao thức cụ thể  
  Chỉ ra loại gói tin mà luật được áp dụng: IP – ICMP – TCP – UDP   
  Nếu là IP thì Snort sẽ kiểm tra header của lớp liên kết để xác định loại gói tin. Nếu bất kỳ giao thức nào khác, Snort sẽ sử dụng header IP để xác định loại giao thức.
* Address: địa chỉ nguồn và địa chỉ đích  
  Mỗi địa chỉ có thể là 1 IP đơn hoặc 1 dải mạng. Nếu là “any” thì áp dụng cho tất cả địa chỉ trong mạng.   
  Snort cung cấp phương pháp để loại trừ địa chỉ IP bằng cách sử dụng dấu ‘!”
* Port: xác định các cổng nguồn, cổng đích của một gói tin  
  Số port để áp dụng cho các luật. Để sử dụng 1 dãy các port thì ta phân biệt bới dấu “:”
* Direction: phần này sẽ chỉ ra đâu là địa chỉ nguồn và đâu là địa chỉ đích dựa theo chiều mũi tên.

### 3.4.2 Rule options

Phần Option nằm ngay sau phần Header và được bao bọc trong dấu ngoặc đơn. Nếu có nhiều option thì sẽ phân biệt nhau bởi dấu “;”. Một option gồm 2 phần: một từ khóa và một tham số, 2 phần này sẽ phân cách nhau bằng dấu hai chấm.

* Từ khóa ack:  
  Trong header TCP có chứa trường Acknowledgement Number với độ dài 32 bit. Trường này chỉ ra số thứ tự tiếp theo gói tin TCP của bên gửi đang được chờ để nhận. Trường này chỉ có ý nghĩa khi mà cờ ACK được thiết lập. Các công cụ như Nmap sử dụng đặc điểm này để ping một máy. Ví dụ nó có thể gửi gói tin TCP tới cổng 80 với cờ ACK được bật và số thứ tự là 0. Bởi vậy bên nhận thấy gói tin không hợp lệ sẽ gửi lại gói tin RST. Và khi nhận được gói RST này, Nmap sẽ biết được IP này đang tồn tại hay không.  
  Để kiểm tra loại ping TCP này thì ta có thể dùng luật sau:  
  alert tcp any any -> 192.168.0.0/22 any (flags: A; ack: 0; msg: “TCP ping detected”)
* Từ khóa classtype:  
  Các luật có thể được phân loại và gán cho 1 số chỉ độ ưu tiên nào đó để nhóm và phân biệt chúng với nhau. Để hiểu rõ hơn về classtype thì ta cần hiểu được file classification.config. Mỗi dòng trong file này đều có cấu trúc như sau:  
  Config classification: name, description, priority  
  Trong đó:  
  Name: tên dùng để phân loại, tên này sẽ được dùng với từ khóa classtype trong các luật Snort  
  Description: mô tả   
  Priority: là 1 số chỉ độ ưu tiên mặc định của lớp này. Độ ưu tiên này có thể được điều chỉnh trong từ khóa priority của phần Option trong Snort  
  VD:  
  Config classification: DoS, Denied of Service Attack, 2  
  Và luật  
  Alert udp any any -> 192.168.0.0/22 6838 (msg:”DoS”; content: “server”; classtype: DoS; priority: 1;)  
  đã ghi đè lên giá trị priority mặc định của lớp đã định nghĩa
* Từ khóa content:   
  Một đặc tính quan trọng của Snort là có khả năng tìm 1 mẫu dữ liệu bên trong một gói tin.  
  VD: alert tcp 192.168.0.0/22 any -> ![192.168.0.0/22] any (content: “GET”; msg :”GET match”  
  Luật trên tìm mãu “GET” trong phần dữ liệu của tất cả gói tin TCP có nguồn mạng là 192.168.0.0/22 đi đến các địa chỉ đích không nằm trong dải mạng đó.  
  Tuy nhiên khi sử dụng từ khóa content cần nhớ rằng:  
  Đối chiếu nội dung cần phải xử lý rất lớn nên ta phải cân nhắc kỹ khi sử dụng nhiều luật đối chiếu nội dung.  
  Các từ khóa được sử dụng cùng với content để bổ sung thêm các điều kiện là:  
  + Offset: dùng để xác định vị trí bắt đầu tìm kiếm là offset tính từ đầu phần dữ liệu của gói tin. VD: alert tcp 192.168.0.0/22 any -> any any (content: “HTTP”; offset: 4; msg: “HTTP matched”  
  + Dept: dùng để xác định vị trí mà từ đó Snort sẽ dừng việc tìm kiếm. VD: alert tcp 192.168.0.0/22 any -> any any (content: “HTTP”; dept: 10; msg: “HTTP matched”
* Từ khóa dsize:  
  Dùng để đối sánh theo chiều dài của phần dữ liệu. Rất nhiều cuộc tấn công sử dụng lỗi tràn bộ đệm bằng cách gửi các gói tin có kích thước rất lớn.  
  VD: alert ip any any -> 192.168.0.0/22 any (dsize > 5000; msg: “Goi tin co kich thuoc lon”)
* Từ khóa flags:  
  Từ khóa này dùng để phát hiện xem những bit cờ flag nào được bật trong phần TCP header của gói tin. Mỗi cờ có thể được sử dụng như 1 tham số trong từ khóa flags.  
  Flag | Kí hiệu tham số dùng trong luật của Snort   
  FIN – Finish Flag | F   
  SYN – Sync Flag | S   
  RST – Reset Flag | R   
  PSH – Push Flag | P   
  ACK – Acknowledge Flag | A   
  URG – Urgent Flag | U   
  Reversed Bit 1 | 1   
  Reversed Bit 2 | 2   
  No Flag set | 0  
  VD: luật sau đây sẽ phát hiện một hành động quét dùng gói tin SYN-FIN:  
  Alert tcp any any -> 192.168.0.0/22 any (flags: SF; msg: “SYNC-FIN flag detected”)
* Từ khóa fragbits:  
  Phần IP header của gói tin chứa 3 bit dùng để chống phân mảnh và tổng hợp các gói tin IP. Các bit đó là:  
  + Reversed bit (RB) dùng để dành cho tương lai  
  + Don’t Fragment Bit (DF): nếu bit này được thiết lập tức là gói tin không bị phân mảnh  
  + More Fragments Bit (MF): nếu được thiết lập thì các phần khác của gói tin vẫn đang trên đường đi mà chưa tới đích. Nếu bit này không được thiết lập thì đây là phần cuối cùng của gói tin.  
  VD: luật sau sẽ phát hiện xem bit DF trong gói tin ICMP có được bật hay không: alert icmp any any -> 192.168.0.0/22 any (fragbits: D; msg: “Don’t Fragment bit set”)

# Chương 4: Chương trình demo bằng Snort

# Tài liệu tham khảo

Tìm hiểu cơ chế và hoạt động của IDS (<https://viblo.asia/p/network-tim-hieu-co-che-cach-hoat-dong-cua-ids-phan-2-pDljMbe5RVZn>)  
Vương Hữu Nhân – Đặng Minh Tuấn: Tìm hiểu và phân tích hoạt động của Snort (<https://www.academia.edu/6535137/Tim_Hieu_Va_Khai_Thac_Dich_Vu_Snort>)