**Chương 1:**

TỔNG QUAN VỀ HỆ THỐNG PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP

*Hệ thống phát hiện xâm nhập đã được sinh ra cách đây 25 năm và đã rất hữu ích trong việc bảo vệ các hệ thống mạng và máy tính. Nó cung cấp cảnh báo khi có dấu hiệu của xâm nhập vào hệ thống. Tuy nhiên, hệ thống IDS vẫn còn nhiều hạn chế và có thể đưa ra những cảnh báo sai, do đó cần có sự giám sát của con người. Thế hệ tiếp theo của IDS là hệ thống IPS đã xuất hiện vào năm 2004 và đang ngày càng phổ biến, thay thế cho các hệ thống IDS. Hệ thống IPS bao gồm các cơ chế phát hiện, cảnh báo và có thể ngăn chặn các hoạt động tấn công bằng cách kết hợp với tường lửa (fire walls).*

**1.1. Hệ thống phát hiện xâm nhập IDS**

* 1. **1. Khái niệm**

Hệ thống phát hiện xâm nhập IDS là một thiết bị phần cứng, phần mềm hoặc cả hai cùng kết hợp để giám sát, theo dõi và thu thập thông tin từ nhiều nguồn khác nhau. Sau đó, thông tin sẽ được phân tích để tìm ra các dấu hiệu của sự xâm nhập hoặc tấn công vào hệ thống và thông báo đến người quản trị hệ thống. Tóm lại, hệ thống IDS là cơ sở để bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn dùng của hệ thống máy tính hoặc hệ thống mạng.

* + 1. **Chức năng**

IDS có tính năng giám sát và bảo vệ lưu lượng mạng khỏi những truy cập trái phép:

* Giám sát và bảo vệ hoạt động của bộ định tuyến, tường lửa, quản lý key và tệp khỏi các cuộc tấn công mạng.
* Hỗ trợ quản lý và thay đổi các đường dẫn, nhật ký và cú pháp.
* Giao diện thân thiện với người dùng.
* Tích hợp các thông tin của cơ sở dữ liệu chữ ký tấn công.
* Phát hiện và báo lỗi bảo mật hoặc thay đổi tệp về hệ thống.
* Ngăn chặn hành vi xâm nhập bằng cách chặn hoặc tắt quyền truy cập.
  + 1. **Kiến trúc của hệ thống phát hiện xâm nhập**

Kiến trúc của một hệ thống phát hiện xâm nhập (IDS) bao gồm ba thành phần chính: thành phần thu thập thông tin (*information collection*), thành phần phát hiện (*detection*) và thành phần phản hồi (*response*). Trong số ba thành phần này, thành phần phát hiện là phần quan trọng nhất và bộ cảm biến **(sensor)** đóng vai trò quan trọng trong quá trình này. Để hiểu rõ hơn về cấu trúc của một hệ thống IDS, ta cần phân tích kỹ hơn về *bộ cảm biến*.

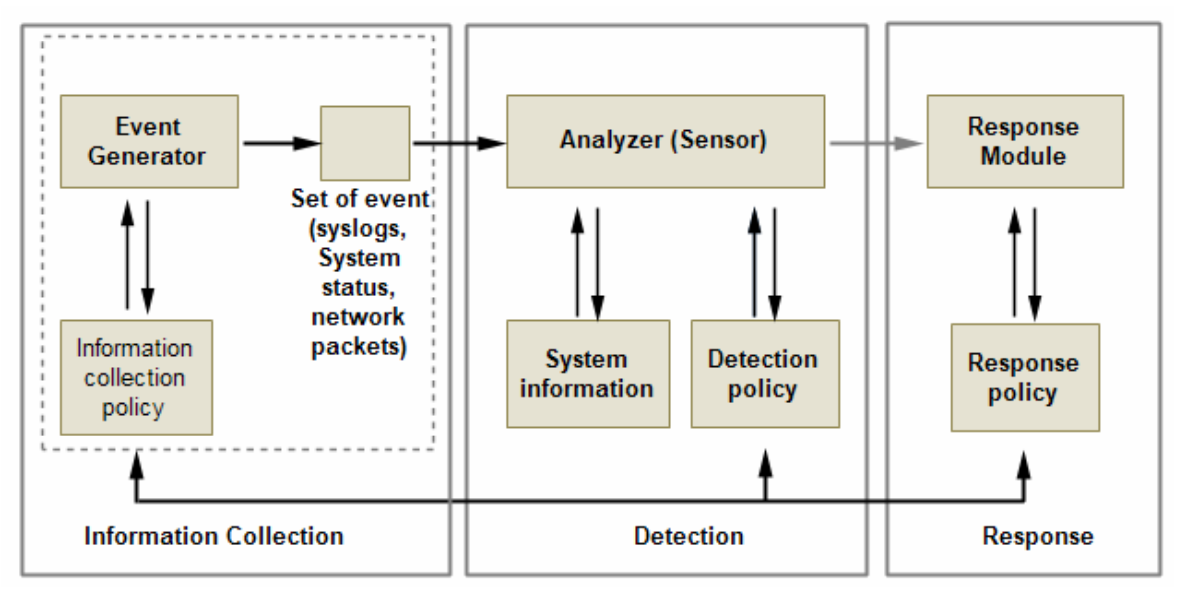


Figure 1. Kiến trúc của một hệ thống phát hiện xâm nhập

Bộ cảm biến được tích hợp với thành phần thu thập dữ liệu và bộ tạo sự kiện. Cách thu thập dữ liệu được xác định bởi chính sách tạo sự kiện để định nghĩa chế độ lọc thông tin sự kiện. Bộ tạo sự kiện (bao gồm hệ điều hành, mạng và ứng dụng) cung cấp các chính sách phù hợp cho các sự kiện, có thể là một bản ghi các sự kiện của hệ thống hoặc các gói mạng. Các chính sách này, cùng với thông tin chính sách, có thể được lưu trữ trong hệ thống bảo mật hoặc bên ngoài.

Vai trò của bộ cảm biến là lọc thông tin và loại bỏ dữ liệu không tương thích từ các sự kiện liên quan đến bảo mật hệ thống, giúp phát hiện các hành động đáng ngờ. Bộ phân tích sử dụng cơ sở dữ liệu chính sách phát hiện để thực hiện chức năng này. Ngoài ra, còn có các thành phần khác như: dấu hiệu tấn công, hồ sơ hành vi thông thường và các tham số cần thiết (ví dụ: ngưỡng). Hơn nữa, cơ sở dữ liệu này còn chứa các thông số cấu hình, bao gồm các chế độ truyền thông với module phản hồi. Bộ cảm biến cũng có cơ sở dữ liệu riêng của nó, lưu trữ dữ liệu về các xâm nhập phức tạp tiềm ẩn (tạo ra từ nhiều hành động khác nhau).

Các hệ thống phát hiện xâm nhập (IDS) có thể được triển khai tập trung (ví dụ như tích hợp vào tường lửa) hoặc phân tán. Một IDS phân tán bao gồm nhiều IDS khác nhau trên một mạng lớn, chúng truyền thông với nhau. Nhiều hệ thống phức tạp áp dụng nguyên tắc cấu trúc một tác nhân, trong đó các module nhỏ được sắp xếp trên một host trong mạng được bảo vệ.

Các tác nhân trong hệ thống phát hiện xâm nhập (IDS) có vai trò kiểm tra và lọc hành động trong khu vực được bảo vệ, có thể phân tích ban đầu và đáp ứng hành động. Các tác nhân hợp tác gửi báo cáo đến máy chủ phân tích trung tâm, là thành phần quan trọng của IDS. IDS phân tán (DIDS) sử dụng nhiều công cụ phân tích tinh vi để phát hiện các cuộc tấn công phân tán. Các tác nhân còn có thể được thiết kế để phát hiện các dấu hiệu của các cuộc tấn công đã biết và di động để phù hợp với nhiều vị trí vật lý. Điều này rất quan trọng trong bảo vệ chống lại các loại tấn công mới.

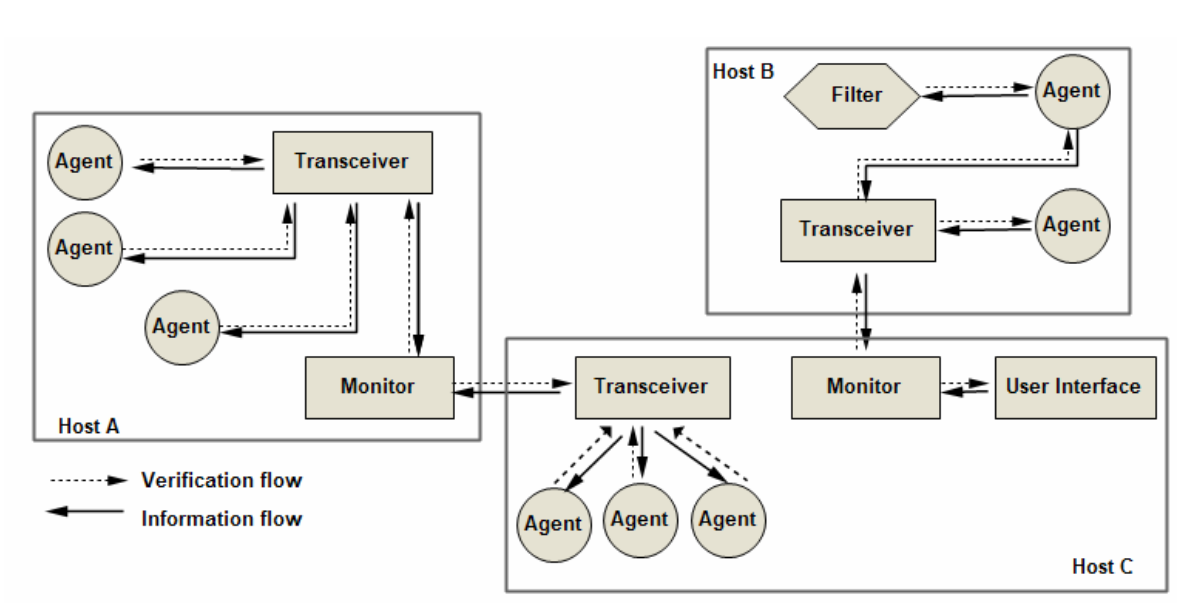
Tác nhân có khả năng cảnh báo khi phát hiện sự kiện khả nghi. Các tác nhân có tính năng tự trị, có thể được sao chép và thay đổi trong các hệ thống khác. Hệ thống có thể có các bộ thu phát để kiểm tra tất cả các hoạt động được kiểm soát bởi các tác nhân trên một host cụ thể. Các bộ thu phát luôn gửi kết quả hoạt động của chúng đến bộ kiểm tra duy nhất. Các bộ kiểm tra nhận thông tin từ các mạng (không phải từ một host), điều đó có nghĩa là chúng có thể tương quan với thông tin phân tán. Ngoài ra, một số bộ lọc có thể được đưa ra để lựa chọn và thu thập dữ liệu.

Figure 2. Giải pháp kiến trúc đa tác nhân

* + 1. **Phân loại hệ thống phát hiện xâm nhập**

Có hai loại hệ thống phát hiện xâm nhập cơ bản là: Network-based IDS và Host-based IDS.

1.1.4.1. Network-based IDS (NIDS)

NIDS là hệ thống phát hiện xâm nhập bằng cách thu thập dữ liệu các gói tin trên các phương tiện truyền dẫn như (cables, wireless) bằng cách sử dụng các card giao tiếp. Khi một gói tin phù hợp với qui tắc của hệ thống, cảnh báo sẽ được tạo ra để thông báo cho nhà quản trị và các tập tin log sẽ được lưu trữ trong cơ sở dữ liệu.

1. Ưu điểm của NIDS

* Quản lý được một phân đoạn mạng (network segment).
* Trong suốt với người sử dụng và kẻ tấn công.
* Cài đặt và bảo trì đơn giản, không ảnh hưởng đến hoạt động của mạng.
* Ngăn chặn các cuộc tấn công dịch vụ đến một host cụ thể.
* Có khả năng phát hiện lỗi tại tầng mạng.
* Độc lập với hệ điều hành.

1. Hạn chế của NIDS

* Có thể báo động giả, khi không có bất kỳ dấu hiệu bất thường nào mà IDS vẫn phát hiện và báo.
* NIDS không thể phân tích được các lưu lượng đã được mã hóa như SSH, IPSec, SSL...
* NIDS cần phải luôn cập nhật các dấu hiệu tấn công mới nhất để hoạt động hiệu quả.
* NIDS không thể xác định được liệu một cuộc tấn công vào mạng có thành công hay không, điều này gây khó khăn cho người quản trị trong việc bảo trì hệ thống.
* Hạn chế về giới hạn băng thông. Các bộ thu thập dữ liệu phải thu thập tất cả các luồng mạng, sắp xếp và phân tích chúng. Tốc độ của bộ thu thập thông tin phải đảm bảo tương ứng với tốc độ của mạng. Giải pháp là đảm bảo mạng được thiết kế chính xác.

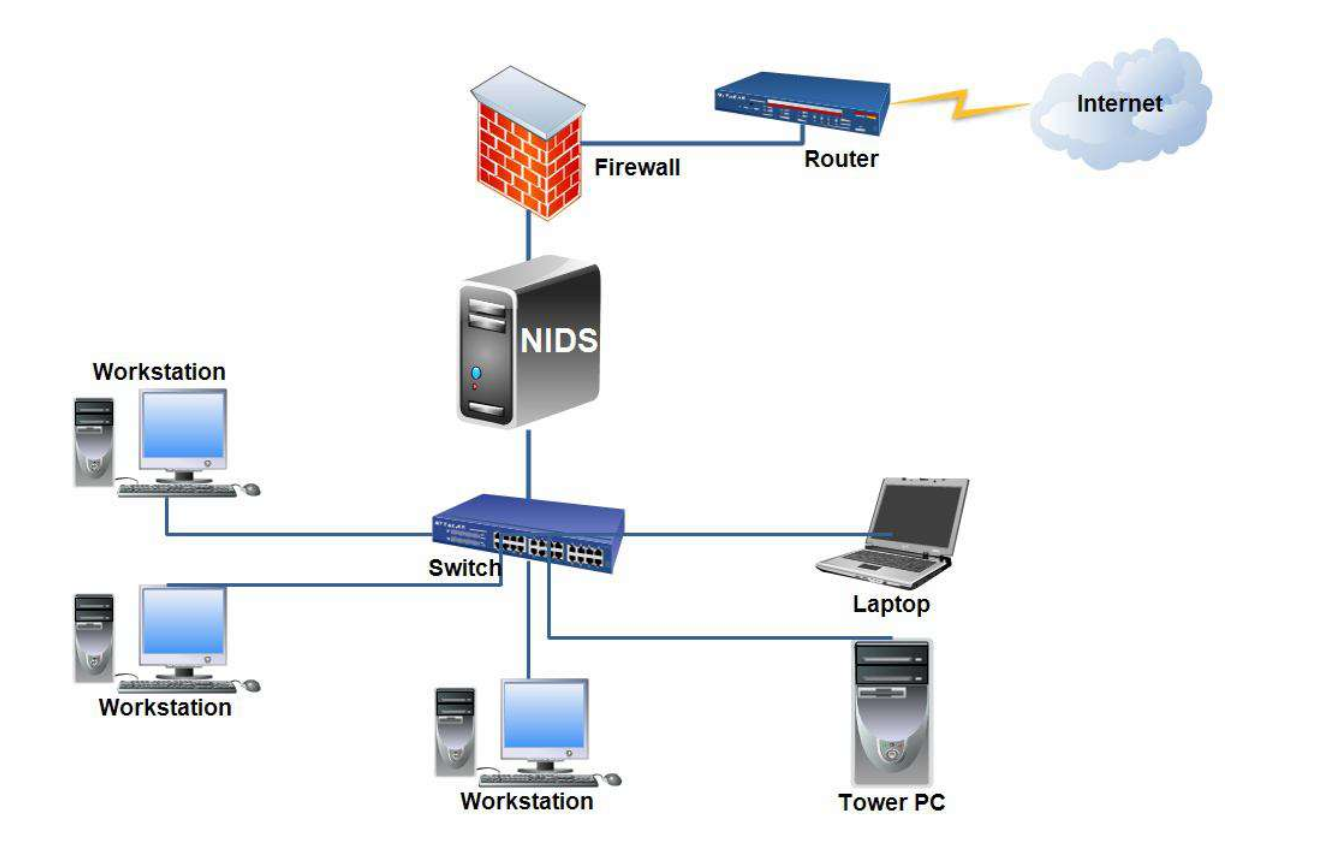
Khi gặp các hệ thống IDS, hacker sẽ sử dụng phân mảnh dữ liệu gói tin để che đậy hoạt động của mình. Phân mảnh là chia nhỏ dữ liệu thành các phần nhỏ hơn, không quan trọng thứ tự nhưng phải tái hợp lại đúng để tránh bị chồng chéo. Hacker sẽ gửi nhiều gói dữ liệu phân mảnh chồng chéo để ngăn chặn phát hiện. Việc sắp xếp gói tin đúng trật tự là rất quan trọng để phát hiện các hoạt động xâm nhập. 

Figure 3. Network-based IDS

1.1.4.2. Host-based IDS (HIDS)

Hệ thống phát hiện xâm nhập trên các máy tính (HIDS) được cài đặt trên nhiều loại máy chủ khác nhau, bao gồm cả máy trạm làm việc hay máy tính xách tay. HIDS linh hoạt hơn NIDS khi có thể hoạt động trên các phân đoạn mạng khác nhau. Nó phân tích và kiểm tra các luồng dữ liệu được gửi đến host và chuyển chúng qua nếu không phát hiện ra các mã độc tiềm ẩn. HIDS cung cấp các chức năng chi tiết hơn cho các ứng dụng và hệ điều hành. Nhiệm vụ chính của HIDS là giám sát sự thay đổi trên hệ thống. HIDS bao gồm các thàng phần chính:

* Các tiến trình.
* Các entry của registry.
* Mức độ sử dụng CPU.
* Kiểm tra tính toàn vẹn và truy cập trên file hệ thống.
* Một vài thông số khác.

Nếu các thông số này vượt quá ngưỡng định trước hoặc thay đổi đáng ngờ, HIDS sẽ phát ra cảnh báo.

1. **Ưu điểm của HIDS**

* Có khả năng xác định người dùng liên quan đến sự kiện trên hệ thống.
* HIDS có thể phát hiện các cuộc tấn công diễn ra trên một máy tính, trong khi NIDS không thể.
* Có khả năng phân tích các dữ liệu đã được mã hóa.
* Cung cấp thông tin chi tiết về host trong khi cuộc tấn công đang diễn ra trên host đó.

1. **Nhược điểm của HIDS**

* Thông tin từ HIDS sẽ không đáng tin cậy ngay sau khi host bị tấn công thành công.
* HIDS không còn hiệu quả khi hệ điều hành bị tấn công.
* HIDS phải được cài đặt trên từng host để giám sát.
* HIDS không thể phát hiện được các hoạt động thăm dò mạng (Nmap, Netcat ...).
* HIDS tốn tài nguyên trên host để hoạt động.
* HIDS có thể không phát hiện được các cuộc tấn công từ chối dịch vụ (DoS).
* Hầu hết các phiên bản HIDS được phát triển trên hệ điều hành Windows, mặc dù cũng có một số phiên bản chạy trên Linux hoặc Unix.

Hệ thống phát hiện xâm nhập dựa trên máy chủ (HIDS) gặp khó khăn khi cần phải cài đặt trên nhiều máy chủ, gây ra sự phức tạp và tốn thời gian khi cần nâng cấp, bảo trì và cấu hình. Ngoài ra, HIDS chỉ phân tích được lưu lượng trên máy chủ, bỏ qua các lưu lượng khác và các hành động thăm dò. Nếu máy chủ bị tấn công, hacker có thể tắt HIDS trên máy đó, khiến nó trở thành vô dụng.

Do đó, HIDS cần cung cấp đầy đủ khả năng cảnh báo trong môi trường hỗn tạp như vậy. Việc lựa chọn HIDS cũng là một vấn đề quan trọng vì nó phải tương thích với nhiều hệ điều hành khác nhau.

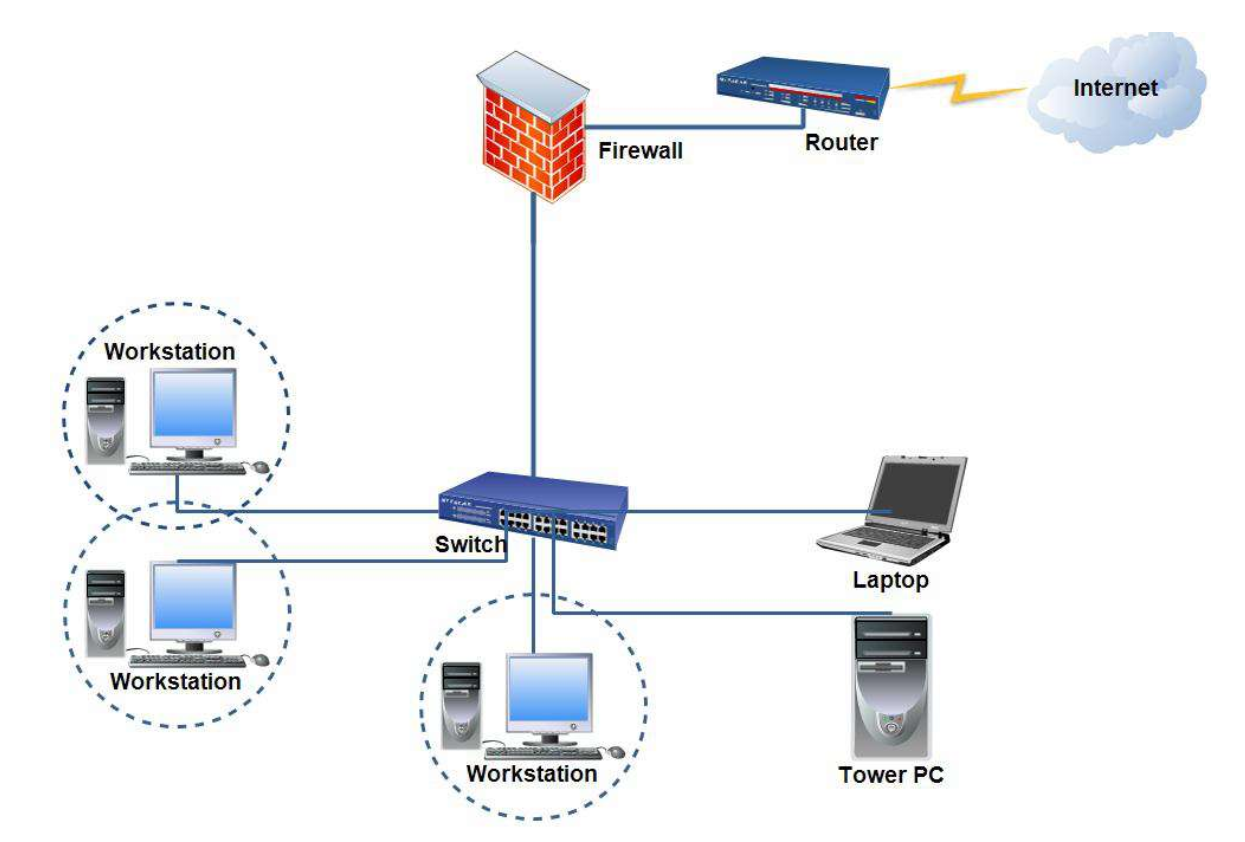


Figure 4. Host-based IDS

**1.2. Hệ thống ngăn chặn xâm nhập IPS**

* + 1. **Khái niệm**

Hệ thống ngăn chặn xâm nhập IPS (Intrusion Prevention System) là một kỹ thuật bảo mật mới, kết hợp các ưu điểm của kỹ thuật firewall và hệ thống phát hiện xâm nhập IDS. Hệ thống này không chỉ phát hiện các cuộc tấn công mà còn có khả năng tự động ngăn chặn chúng.

IPS không chỉ dừng lại ở việc phát hiện tấn công mà còn cho phép tổ chức ưu tiên và thực hiện các bước ngăn chặn tấn công một cách chủ động. Thường thì các hệ thống IPS được đặt ở vị trí ở vành đai mạng, đảm bảo bảo vệ tất cả các thiết bị trong mạng.

* + 1. **Thành phần của hệ thống phát hiện xâm nhập**

Một hệ thống IPS gồm có 3 module chính:

* Module phân tích gói tin.
* Module phát hiện tấn công.
* Module phản ứng.

**1.2.2.1. Module phân tích gói tin**

Nhiệm vụ của module này là phân tích cấu trúc thông tin của gói tin. NIC Card trên máy tính sẽ được cài đặt ở chế độ *promiscuous mode* để giám sát, tất cả các gói tin thông qua chúng sẽ được sao chép và chuyển lên lớp trên. Bộ phân tích gói tin sẽ đọc thông tin từng trường trong gói tin, xác định kiểu gói tin, dịch vụ và loại giao thức được sử dụng. Các thông tin này sẽ được chuyển lên module phát hiện tấn công.

**1.2.2.2. Module phát hiện tấn công**

Module này là một trong những module quan trọng nhất trong hệ thống phát hiện xâm nhập, có khả năng phát hiện các cuộc tấn công. Có nhiều phương pháp để phát hiện dấu hiệu xâm nhập hoặc các loại tấn công như IPS dựa trên chữ ký (signature-based IPS), IPS dựa trên bất thường (anomaly-based IPS),...

* **Phương pháp dò Misuse Detection (sự lạm dụng):** Phương pháp này phân tích các hoạt động của hệ thống, tìm kiếm các sự kiện giống với các mẫu tấn công đã biết trước. Các mẫu tấn công biết trước này gọi là các dấu hiệu tấn công. Do vậy phương pháp này còn được gọi là phương pháp dò dấu hiệu. Kiểu phát hiện tấn công này có ưu điểm là phát hiện các cuộc tấn công nhanh và chính xác, không đưa ra các cảnh báo sai làm giảm khả nǎng hoạt động của mạng và giúp các người quản trị xác định các lỗ hổng bảo mật trong hệ thống của mình. Tuy nhiên, phương pháp này có nhược điểm là không phát hiện được các cuộc tấn công không có trong cơ sở dữ liệu, các kiểu tấn công mới, do vậy hệ thống luôn phải cập nhật các mẫu tấn công mới.
* **Phương pháp Anomaly Detection (dò sự không bình thường):** Đây là kỹ thuật sử dụng một mô hình dựa trên học máy để phát hiện các hoạt động không bình thường trên mạng. Mô hình này được đào tạo để xác định các mẫu hoạt động bình thường, và khi các hoạt động mới không khớp với các mẫu này, hệ thống sẽ cảnh báo người quản trị để xem xét và xác định liệu các hoạt động đó có phải là một cuộc tấn công hay không.Anomaly Detection có thể phát hiện các cuộc tấn công mới hoặc chưa biết trước, nhưng cũng có thể gây ra nhiều sai sót do không phân biệt được các hoạt động không bình thường đáng kể với các hoạt động thông thường.

**1.2.2.3. Module phản ứng**

Khi module phát hiện tấn công phát hiện được dấu hiệu của cuộc tấn công hoặc xâm nhập, nó sẽ gửi tín hiệu báo hiệu cho module phản ứng. Sau đó, module phản ứng sẽ kích hoạt firewall để thực hiện chức năng ngăn chặn cuộc tấn công. Tại module này, nếu chỉ đưa ra các cảnh báo cho các nhân viên quản trị và dừng lại ở đó thì hệ thống này được gọi là hệ thống phòng thủ bị động. Tuy nhiên, module phản ứng này có thể có các chức năng khác nhau tùy thuộc vào từng hệ thống. Dưới đây là một số kỹ thuật ngăn chặn được sử dụng:

* Terminate session:

Kỹ thuật này của hệ thống IPS gửi gói tin reset để thiết lập lại cuộc giao tiếp giữa client và server, làm cho mục đích của hacker không được đạt được và ngừng cuộc tấn công. Tuy nhiên, phương pháp này có nhược điểm là thời gian gửi gói tin reset đến đích quá lâu so với thời gian gói tin của hacker đến Victim, dẫn đến reset quá chậm so với cuộc tấn công. Ngoài ra, phương pháp này không hiệu quả đối với các giao thức hoạt động trên UDP như DNS. Gói tin Reset phải có trường sequence number đúng (so với gói tin trước đó từ client) thì server mới chấp nhận, do đó nếu hacker gửi các gói tin với tốc độ nhanh và trường sequence number thay đổi thì khó thực hiện được phương pháp này.

* Drop attack:

Kỹ thuật này sử dụng firewall để hủy bỏ hoặc chặn gói tin hoặc một luồng thông tin giữa hacker và victim. Đây là phản ứng an toàn nhất nhưng có thể nhầm lẫn với các gói tin hợp lệ.

* Modify firewall polices

Kỹ thuật này cho phép người quản trị cấu hình lại chính sách bảo mật khi cuộc tấn công xảy ra. Sự cấu hình lại là tạm thời thay đổi các chính sách điều khiển truy cập bởi người dùng đặc biệt trong khi cảnh báo tới người quản trị.

* Real-time Alerting:

Gửi cảnh báo thời gian thực đến người quản trị để họ nắm bắt chi tiết cuộc tấn công và thông tin về chúng.

* Log packet:

Dữ liệu của các gói tin sẽ được lưu trữ trong hệ thống các file log để theo dõi các luồng thông tin và là nguồn thông tin hỗ trợ cho module phát hiện tấn công hoạt động.

🡪 Ba module trên hoạt động tuần tự tạo nên hệ thống IPS hoàn chỉnh. Một hệ thống IPS được xem là thành công nếu có thể thực hiện nhanh, chính xác, đưa ra các thông báo hợp lý, phân tích toàn bộ thông lượng, cảm biến tối đa, ngăn chặn thành công và có chính sách quản lý mềm dẻo. Với sự phát triển của các kiểu tấn công mới, hệ thống IPS trở thành không thể thiếu trong các hệ thống bảo mật.

**1.2.3. Phương pháp ngăn chặn xâm nhập**

**1.2.3.1. Signature-based IPS**

Signature-based Intrusion Prevention System (IPS) là một hệ thống dùng để phát hiện và ngăn chặn các cuộc tấn công bằng cách tạo ra các quy tắc (hay còn gọi là signature). Signature-based IPS giám sát lưu lượng mạng và tìm kiếm các mẫu tấn công khớp với các signature đã tạo trước đó. Các signature này là các mẫu tấn công được định cấu hình trước để phát hiện các hoạt động xâm nhập thông thường. Những nghiên cứu về các kỹ thuật tấn công, mẫu và phương pháp để viết ra các signature được sử dụng để cập nhật các file signature. Khi có thêm các kỹ thuật tấn công mới hoặc các phương pháp khai thác mới được phát hiện, nhà cung cấp signature sẽ cập nhật file signature tương ứng.

Khi phát hiện một mẫu tấn công phù hợp với các signature đã biết, hệ thống sẽ kích hoạt và đưa ra cảnh báo cho người quản trị để họ có thể ngăn chặn hoặc phản ứng lại tấn công đó.

-Ưu điểm của Signature-based Intrusion Prevention System (IPS):

+ Tính đơn giản: Hệ thống IPS dựa trên signaturecó thể dễ dàng cài đặt và quản lý vì nó dựa trên các signatuređã biết và được cấu hình trước.

+ Hiệu quả trong việc phát hiện các cuộc tấn công đã biết: Với các mẫu tấn công đã biết được định cấu hình trước, hệ thống IPS dựa trên signaturecó thể phát hiện các cuộc tấn công này một cách hiệu quả.

+ Bảo vệ ngay lập tức: Vì các signatuređã được định cấu hình trước, hệ thống IPS dựa trên signaturecó thể ngăn chặn các cuộc tấn công có signaturemột cách nhanh chóng và hiệu quả.

+ Tính khả dụng cao: Hệ thống IPS dựa trên signaturecó thể được triển khai trên nhiều hệ thống và môi trường mạng khác nhau.

+ Hiệu quả với các cuộc tấn công đơn giản: Với các cuộc tấn công đơn giản và có signaturerõ ràng, hệ thống IPS dựa trên signaturecó thể phát hiện và ngăn chặn chúng một cách hiệu quả.

-Nhược điểm của Signature-based Intrusion Prevention System (IPS):

+ Không thể phát hiện các cuộc tấn công mới: Với các cuộc tấn công mới chưa được đưa vào CSDL, hệ thống IPS dựa trên signature không thể phát hiện chúng.

+ Không có khả năng phát hiện những sự thay đổi của những cuộc tấn công đã biết : Những file dấu hiệu là những file tĩnh tức là chúng không thích nghi với một vài hệ thống dựa trên sự bất thường. Bằng cách thay đổi cách tấn công, một kẻ xâm nhập có thể thực hiện cuộc xâm nhập mà không bị phát hiện(false negative).

+ Có thể tạo ra các báo động giả: Nếu hệ thống IPS dựa trên signature được cấu hình không chính xác, nó có thể phát ra các báo động giả hoặc bỏ sót các cuộc tấn công quan trọng.

**1.2.3.2. Anomaly-based IPS**

Anomaly-based Intrusion Prevention System (IPS) là một phần mềm hoặc thiết bị phần cứng được sử dụng để phát hiện và ngăn chặn các hành vi tấn công trên hệ thống mạng. Anomaly-based IPS khác với Signature-based IPS bởi vì nó không dựa trên các quy tắc định sẵn để phát hiện các mẫu tấn công đã biết. Thay vào đó, nó sử dụng thuật toán máy học và học máy để phân tích các hoạt động mạng và đánh giá xem chúng có bất thường hay không. Sự bất thường là bất cứ sự chệch hướng hay đi khỏi những thứ tự, dạng, nguyên tắc thông thường. Nó có thể bao gồm các yêu cầu truy cập không hợp lệ, sử dụng các dịch vụ mạng không phù hợp hoặc có kích thước lớn hơn bình thường, và các yêu cầu gửi thông tin đăng nhập không hợp lệ. Chính vì dạng phát hiện này tìm kiếm những bất thường nên nhà quản trị bảo mật phải định nghĩa đâu là những hoạt động, lưu lượng bình thường. Nhà quản trị bảo mật có thể định nghĩa những hoạt động bình thường bằng cách tạo ra những bản mô tả sơ lược nhóm người dùng (user group profiles).

Anomaly-based IPS cũng có thể sử dụng một số kỹ thuật phân tích dữ liệu để xác định các đặc điểm của các hành vi bất thường. Ví dụ, họ có thể phân tích các yêu cầu mạng để xác định thời gian trung bình giữa các yêu cầu hoặc lượng dữ liệu truyền tải trung bình trong một khoảng thời gian cụ thể. Bằng cách so sánh các yêu cầu và dữ liệu thực tế với các giá trị trung bình này, Anomaly-based IPS có thể phát hiện các hành vi bất thường và ngăn chặn các tấn công từ xa.

-Ưu điểm của Anomaly-based Intrusion Prevention System (IPS):

+Có khả năng phát hiện và ngăn chặn các cuộc tấn công mới và chưa biết trước được bằng cách so sánh với các hành vi bình thường hoặc mẫu độc hại đã biết trước đó.

+Không cần phải cập nhật liên tục như signature-based IPS, do đó không bị giới hạn bởi khả năng phát hiện các cuộc tấn công có mẫu mới.

+Có thể học được các hành vi mới và tự động điều chỉnh để phát hiện các mẫu tấn công mới.

-Tuy nhiên, Anomaly-based IPS cũng có một số nhược điểm:

+Có thể xảy ra sai sót phát hiện giả và báo động sai, khi một hành vi bình thường bất thường được xem như là một cuộc tấn công.

+Khả năng phát hiện và ngăn chặn các cuộc tấn công mà đã được biết trước là hạn chế, vì các tấn công này có thể được thiết kế để tránh phát hiện bằng cách giảm thiểu các hành vi không bình thường.

+Có thể mất nhiều thời gian để xác định một hành vi bất thường là một cuộc tấn công thực sự, do đó có thể làm giảm hiệu quả của hệ thống trong việc ngăn chặn các cuộc tấn công.

**1.2.3.3. Policy-Based IPS**

Policy-Based Intrusion Prevention System (IPS) là một hình thức phát hiện và ngăn chặn xâm nhập dựa trên chính sách (policy) được thiết lập bởi người quản trị. Policy-Based IPS hoạt động bằng cách so sánh các hoạt động trong mạng với các quy tắc được thiết lập trước, bao gồm các giao thức, port, và các quy tắc hành vi. Nếu một hoạt động nào đó vi phạm với các quy tắc được thiết lập, Policy-Based IPS sẽ thực hiện hành động như cắt kết nối hoặc chặn gói tin đó.

Policy-Based IPS có thể được sử dụng để giám sát và quản lý các chính sách bảo mật trong một tổ chức. Nó cho phép quản trị viên quản lý các quy tắc bảo mật tập trung và áp dụng chúng cho tất cả các thiết bị mạng trong hệ thống.

-Ưu điểm của Policy-Based IPS:

+Hiệu quả cao trong việc phát hiện và ngăn chặn các cuộc tấn công đã biết trước hoặc các hành vi có thể gây nguy hiểm cho hệ thống.

+Cung cấp khả năng kiểm soát linh hoạt, xác thực,phản ứng nhanh và rất ít có những cảnh báo sai thông qua việc thiết lập các quy tắc và chính sách bảo mật phù hợp,chính xác với tổ chức.

+Không yêu cầu nhiều tài nguyên máy tính để triển khai và hoạt động, do đó có thể giảm chi phí đầu tư cho hệ thống bảo mật.

-Nhược điểm của Policy-Based IPS:

+Không phát hiện được các cuộc tấn công mới, chưa biết trước hoặc các hành vi bất thường không thuộc quy tắc đã được thiết lập sẵn.

+Dễ bị đánh lừa khi kẻ tấn công sử dụng các kỹ thuật lừa đảo như tấn công từ chối dịch vụ (DoS) hay các kỹ thuật đánh lừa khác để vượt qua chính sách bảo mật.

+Thiết lập và duy trì các chính sách bảo mật phù hợp với môi trường mạng của tổ chức có thể đòi hỏi nhiều thời gian và công sức, đặc biệt là khi hệ thống mạng phức tạp hoặc có nhiều quy tắc cần phải thiết lập.

**1.2.3.4. Protocol Analysis IPS**

Protocol Analysis IPS (Intrusion Prevention System) là một loại hệ thống chống xâm nhập cũng tương tự như Signature-Based IPS nhưng dựa trên việc phân tích các giao thức mạng. Nó hoạt động bằng cách kiểm tra các giao thức được sử dụng trong mạng, phát hiện và ngăn chặn các hành vi xâm nhập không hợp lệ, như các gói tin chứa mã độc hoặc các lỗ hổng bảo mật được sử dụng để khai thác các thiết bị mạng.

-Ưu điểm khi sử dụng Protocol Analysis IPS:

+Phát hiện được các cuộc tấn công mới: Protocol Analysis IPS dựa trên việc phân tích các giao thức mạng để phát hiện các cuộc tấn công mới, không giống như các hệ thống dựa trên signaturechỉ có thể phát hiện các cuộc tấn công đã biết trước.

+Có thể xử lý được các cuộc tấn công nâng cao: Protocol Analysis IPS có thể phát hiện các cuộc tấn công phức tạp hơn, bao gồm cả các cuộc tấn công mà các hệ thống IPS khác không thể phát hiện được.

-Nhược điểm khi sử dụng Protocol Analysis IPS:

+Số lượng thông tin phải xử lý lớn: Protocol Analysis IPS phải phân tích các giao thức mạng để phát hiện các cuộc tấn công, do đó nó phải xử lý một lượng lớn thông tin mạng, đôi khi có thể gây ra hiện tượng giảm hiệu suất.

+Có thể phát hiện nhầm các cuộc tấn công: Các hệ thống Protocol Analysis IPS có thể phát hiện nhầm các cuộc tấn công trong trường hợp các giao thức mạng bị lỗi hoặc nhiễu sóng mạng. Điều này có thể dẫn đến việc phát hiện giả hoặc báo động sai.