**Hoạt động của IDS**

1. **Kiến trúc và chức năng**



Thành phần thu thập gói tin: Các cảm biến

Thành phần phân tích và báo hiệu: các mẫu để so sánh với thông tin thu được.

Thành phần phản hồi: phản ứng khi gói tin được phát hiện ra là một nguy cơ.

Hệ thống IDS hoạt động theo cơ chế so sánh thông tin thu được với mẫu. Đầu tiên, cảm biến tiến hành bắt các gói tin và rồi đọc nội dung cũng như so sánh các xâu trong đó với các mẫu tín hiệu đã nhận biết. Trong trường hợp giống nhau, thì các gói tin được đánh dấu là bình thường, ngược lại sẽ là có dấu hiệu tấn công. Những tín hiệu phát hiện các cuộc tấn công được tổng hợp lại thành bộ - signatures. Mẫu ở đây được sinh ra dựa trên kinh nghiệm.

Trong kiến trúc IDS, thành phần ở giữa phát hiện, phân tích gói tin là quan trọng nhất và ở thành phần này, bộ cảm biến đóng vai trò quyết định. Bộ cảm biến kết nối các thành phần bằng chính sách tạo sự kiện nhằm nêu lên khái niệm về chế độ lọc thông tin sự kiện. Bộ cảm biến được sử dụng trong việc lọc thông tin, bỏ qua dữ liệu không phù hợp có được từ những sự kiện liên quan đến hệ thống được bảo vệ, từ đó phát hiệt các dấu hiệu đáng ngờ. Bộ phân tích sẽ dùng cơ sở dữ liệu chính sách tìm thấy cho mục này. Đồng thời còn có thêm thành phần: dấu hiệu tấn công, mô tả hành vi bình thường, các tham số khác.

Hai kỹ thuật cơ bản:

* Dựa vào dấu hiệu
* Dựa vào bất thường

Quy trình chung:

* Máy chủ tạo gói tin.
* Trước khi gói tin được gửi, cảm biến đọc trước gói tin.
* Chương trình phát hiện nằm bên trong cảm biến, kiểm tra các gói. Nếu có vi phạm, ngay lập tức cảnh báo tới điều khiển.
* Tại giao diện điều khiển, nhận được cảnh báo, bộ công cụ gửi thông báo tới các cá nhân (nhóm) có thẩm quyền.
* Cảnh báo được lưu log.
* Cảnh báo được đối chiếu với dữ kiện khác.

Quy tắc tiêu đề:

* Hoạt động: cung cấp các hành động thêm khi luật thông qua
* Giao thức: giao thức sẽ kiểm tra
* IP
* Cổng
* Hướng

Quy tắc tùy chọn:

* General:
* Payload:
* Non-payload
* Phát hiện sau

Những điều kiện cần phải thỏa mãn của một hệ thống phát hiện xâm nhập:

* Hiệu năng: Đầu tiên phải thỏa mãn về hiệu năng, phải đủ để phát hiện xâm nhập trong thời gian thực. Điều này đồng nghĩa với việc hành động xâm nhập không cho phép phải được phát hiện ra trước khi những tổn hại nghiêm trọng xảy ra.
* Tính chính xác: Phải hạn chế những hành động thông thường nhưng bị coi là bất thường. IDS cần phân biệt được hành động bất thường và các hành động thông thường của hệ thống.
* Tính trọn vẹn: Phải chắc chắn rằng IDS sẽ không bỏ qua một xâm nhập trái phép nào trong hệ thống. Việc bỏ qua những vụ xâm nhập trái phép gọi là âm tính giả.
* Khả năng mở rộng: IDS cần có khả năng không bỏ sót thông tin dù ở trạng thái xấu nhất. Yêu cầu này thường sẽ liên quan trực tiếp đến hệ thống khi có những sự kiện tương quan đến từ những nguồn tài nguyên có số lượng host nhỏ. Còn trong sự phát triển mạnh mẽ của IoT thì hệ thống sẽ gặp phải quá tải do sự gia tăng số lượng lớn những sự kiện.
* Chịu lỗi: Một yêu cầu hết sức cần thiết chính là bản thân IDS phải có khả năng chống lại được tấn công.

Những chức năng chính của IDS:

* IDS sẽ cung cấp một cách nhìn tổng thể về lưu lượng mạng, có chức năng giám sát thành phần cần bảo vệ trong hệ thống trước các hoạt động bất thường.
* IDS cần phân tích hành vi truy cập, hoạt động, sự kiện quan trọng liên quan đến thành phần được giám sát dựa vào những hành vi bất thường, tập luật, baseline xem đó là hoạt động xâm nhập hay tấn công hệ thống
* IDS mang đến những cảnh báo hiểm họa an toàn thông tin. Thay vì dùng những thiết lập mặc định thì cần nâng cao hơn để chống lại kẻ xâm nhập.
* IDS cũng phải thống kê và trích xuất báo cáo.

1. **Kỹ thuật phát hiện xâm nhập dựa vào dấu hiệu**

A diagram of a computer

Description automatically generated

Độ chính xác của hệ thống tương đối cao, giảm tối thiểu số lượng báo động giả, phát hiện được các hành vi tấn công phức tạp. Tuy nhiên, nhược điểm phổ biến của IDS dựa trên dấu hiệu là: quá tải gói mạng, chi phí khớp chữ ký cao và số lượng báo động sai lớn. Bên cạnh đó, việc bị hạn chế bộ nhớ nghiêm trọng trong một vài mạng như mạng cảm biến không dây (WSN), có thể dẫn đến hiệu suất thấp của IDS (dựa trên nhu cầu cần lưu trữ cơ sở dữ liệu lớn về chữ ký tấn công). Đồng thời, cần phải cập nhật liên tục IDS phù hợp với mẫu, cơ sở dữ liệu chữ ký và mẫu trong IDS dựa vào chữ ký. IDS dựa trên dấu hiệu này được thiết kế nhằm phát hiện các cuộc tấn công, xâm nhập độc hại dựa vào kiến thức trước đó.

1. **Kỹ thuật phát hiện xâm nhập dựa vào bất thường**

Các hành động bất thường sẽ được phát hiện cho việc xác định những cuộc tấn công, đặc biệt là với các cuộc tấn công chưa biết. IDS dựa vào sự bất thường sẽ hoạt động bằng cách tạo ra một mô hình hành vi bình thường trong môi trường máy tính đã được cập nhật liên tục và dựa trên dữ liệu của người dùng bình thường, sau đó sử dụng mô hình này để phát hiện ra bất cứ sai sót nào so với các hành vi bình thường.

Phát hiện xâm nhập dựa vào sự bất thường sẽ phân tích dựa trên các thuật toán thông minh và cũng sẽ hoạt động tùy vào môi trường, hỗ trợ phát hiện những biến cố bất thường. Đồng thời, dựa vào các hoạt động thường nhật của hệ thống để tự động phát hiện ra những điều bất thường và dò tìm xem nó sẽ thuộc vào dạng tấn công nào. Các kỹ thuật phát hiện xâm nhập dựa vào sự bất thường bao gồm: phát hiện bất thường dựa trên học máy, phát hiện bất thường dựa trên dấu vết…

A diagram of a computer network

Description automatically generated