**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**A logo with a star

Description automatically generated**

**Kiến trúc và giao thức IoT**

**Hệ thống phát hiện xâm nhập IDS**

|  |  |
| --- | --- |
| Nhóm sinh viên: | |
| Hoàng Thành Long | B20DCVT233 |
| Tạ Văn An | B20DCVT009 |
| Trần Thị Ánh | B20DCVT042 |
| Vi Xuân Trường | B20DCVT410 |

1. **Giới thiệu về IDS**
2. **IDS là gì?**

IDS (Intrusion Detection System) – Hệ thống phát hiện xâm nhập là một công cụ bảo mật mạng. IDS giám sát lưu lượng và các thiết bị mạng để phát hiện hoạt động độc hại đã biết, hoạt động đáng ngờ hoặc hoạt động vi phạm chính sách bảo mật.

IDS có thể giúp tăng tốc và tự động hóa việc phát hiện mối đe dọa mạng bằng cách cảnh báo cho quản trị viên bảo mật về các mối đe dọa đã biết hoặc tiềm ẩn hoặc bằng cách gửi cảnh báo đến một công cụ bảo mật tập trung. Một công cụ bảo mật tập trung như hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) có thể kết hợp dữ liệu từ các nguồn khác để giúp các nhóm bảo mật xác định và ứng phó với các mối đe dọa mạng có thể sảy ra.

IDS không thể tự mình ngăn chặn các mối đe dọa bảo mật. Ngày nay, các khả năng của IDS thường được tích hợp với các hệ thống ngăn chặn xâm nhập (IPS) để có thể phát hiện các mối đe dọa bảo mật và tự động hành động để ngăn chặn chúng.

1. **IDS hoạt động như thế nào?**

IDS có thể là các ứng dụng phần mềm được cài đặt trên thiết bị đầu cuối hoặc các thiết bị phần cứng chuyên dụng được kết nối với mạng. Một số giải pháp IDS có sẵn dưới dạng dịch vụ đám mây. Dù ở dạng nào, IDS đều sử dụng một hoặc cả hai phương pháp phát hiện mối đe dọa chính: phát hiện dựa trên dấu hiệu hoặc dựa trên sự bất thường.

1. **Một số loại IDS phổ biến**

Có nhiều loại IDS khác nhau đi kèm những chức năng và nhiệm vụ riêng biệt như:

* NIDS – Hệ thống phát hiện xâm nhập mạng được đặt tại những điểm dễ bị tấn công trong hệ thống và có nhiệm vụ giám sát lưu lượng đến và đi từ các thiết bị trên mạng.
* Snort – Hệ thống xâm nhập mạng NIDS mã nguồn mở hoạt động miễn phí trên các hệ điều hành như Unix, Linux và Windows.
* HIDS – Hệ thống phát hiện xâm nhập máy chủ hoạt động trên mọi thiết bị máy tính được kết nối với internet giúp phát hiện và xử lý các lưu lượng truy cập trái phép trên hệ thống.
* SIDS – Hệ thống phát hiện xâm nhập hoạt động dựa trên chữ ký, có nhiệm vụ giám sát các gói dịch vụ trên mạng giống như cách phần mềm diệt virus hoạt động.
* AIDS – Hệ thống phát hiện các xâm nhập đáng ngờ có nhiệm vụ giám sát lưu lượng mạng và so sánh với mức cơ sở đã được thiết lập sẵn như băng thông, giao thức, cổng và một số thiết bị khác được kết nối với nhau. Nếu phát hiện ra những xâm nhập lạ trên hệ thống, AIDS lập tức báo về cho người dùng thông qua mô hình mở rộng.
* IDS thụ động có chức năng phát hiện và gửi cảnh báo các hành vi xâm nhập gây hại về hệ thống nhưng sẽ không thực hiện xử lý.
* IDS chủ động có nhiệm vụ phát hiện và xử lý xâm nhập gây hại bằng cách chặn địa chỉ IP hoặc tắt quyền truy cập vào các tài nguyên bị hạn chế.

1. **Lợi ích của IDS, ưu nhược điểm và so sánh IDS với các phương pháp bảo mật khác**
2. **Lợi ích của IDS**

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. **Ưu nhược điểm của IDS**

Về ưu điểm

* IDS thích hợp sử dụng cho việc thu thập dữ liệu và bằng chứng của các cuộc tấn công mạng. Nhờ đó việc kiểm tra, điều tra và xử lý sự cố phát sinh dễ dàng, chính xác và kịp thời nhất.
* IDS giúp người dùng có cái toàn diện về hệ thống lưu lượng mạng. Bất cứ hoạt động khả nghi nào đều có thể được phát hiện nhanh chóng nhất.
* IDS giúp người dùng phòng ngừa, phản ứng kịp thời để có biện phát chống lại lại các hoạt động tấn công bất ngờ có thể diễn ra trên hệ thống mạng.
* Các số liệu, thông tin IDS ghi chép, lưu trữ có thể được sử dụng để nâng cao chất lượng hệ thống bảo mật. Chúng cũng là cơ sở để đánh giá rủi ro các cuộc tấn công mạng trong tương lai.

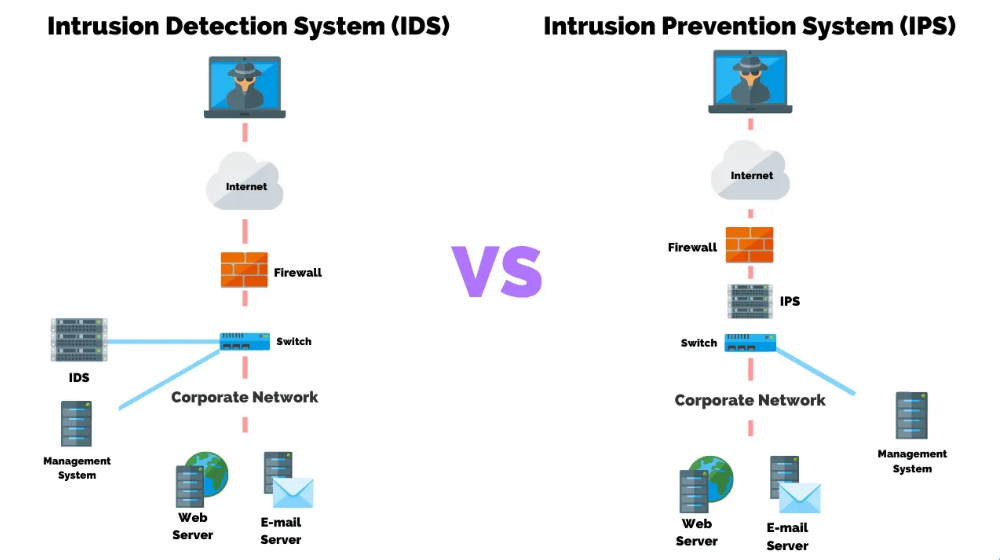
Về nhược điểm

* Người dùng cần điều chỉnh cấu hình IDS phù hợp nếu không sẽ xảy ra tình trạng báo động nhầm, báo động giả.
* Một số hệ thống IDS ngăn cản người dùng ở thiết bị khác truy cập vào hệ thống mạng. Khả năng phân tích lưu lượng traffic mã hóa khá thấp và chưa hiệu quả.
* Chi phí cài đặt hệ thống ISD khá cao và yêu cầu nhiều kỹ thuật phức tạp. Bạn cần cân nhắc nếu khả năng tài chính của doanh nghiệp hạn chế.

1. **So sánh IDS với IPS**

Trước tiên, IDS là một hệ thống phân tích lưu lượng mạng để tìm các thông tin khớp với những mẫu tấn công đã biết trước. Mặt khác, IPS có khả năng phân tích các packet và ngăn chặn việc gửi packet dựa trên những loại hình tấn công mà hệ thống phát hiện được. Từ đó có thể nhanh chóng ngăn chặn tấn công vào hệ thống.

Cả IDS lẫn IPS đều thuộc về cơ sở hạ tầng mạng, và đều so sánh các packet mạng với một CSDL cyberthreat có chứa những signature đã biết của tấn công mạng. Sau đó đánh dấu mọi packet khớp với các mẫu đã biết và cảnh báo cho admin hệ thống.



Sự khác biệt chính giữa hai giải pháp là: IDS là một hệ thống giám sát, còn IPS là hệ thống kiểm soát. IDS không thay đổi các packet mạng, còn IPS ngăn chặn việc gửi packet dựa trên nội dung của nó. Về nguyên lý hoạt động thì IPS tương tự như các tường lửa (tường lừa chặn lưu lượng bằng địa chỉ IP).

* IDS: Phân và giám sát lưu lượng mạng để tìm các dấu hiệu của tấn công mạng. Hệ thống này so sánh các hoạt động mạng hiện tại với CSDL có sẵn để xác định các hành vi đáng ngờ như: vi phạm chính sách, malware hay port scanner.
* IPS: Nằm trong cùng khu vực của firewall trên cơ sở hạ tầng (giữa môi trường bạn ngoài ra mạng ở trong). IPS chủ động chặn các lưu lượng dựa trên một cấu hình bảo mật cụ thể.

Hầu hết các nhà cung cấp dịch vụ IDS/IPS đều tích hợp những hệ thống IPS mới kèm theo firewall để thiết lập công nghệ UTM (Unified Threat Management) – có khả năng kết hợp chức năng của IDS và IPS thành một đơn vị duy nhất.

Nói chung, cả IDP và IPS đều đọc các packet mạng và so sánh nội dung với một CSDL có sẵn. Những điểm khác biệt chỉ nằm ở quá trình sau đó: IDS sẽ phát hiện và giám sát lưu lượng mà không tự thực hiện hành động cụ thể nào cả.

Còn IPS – một hệ thống kiểm soát – sẽ quyết định việc nhận hay bỏ packet mạng dựa trên những bộ quy tắc cho trước. Vì vậy, IDS cần có một người hay hệ thống khác giám sát kết quả và xác định các hành động cần thực hiện.

Tuy nhiên, cần lưu ý rằng IDS/IPS chỉ thực sự hiệu quả nếu có một bộ CSDL đủ tốt. Do đó hãy luôn cập nhật thêm dữ liệu và các bộ quy tắc mới cho CSDL của mình để bảo vê hệ thống tốt nhất.

1. **Hoạt động của IDS**
2. **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