1. DỰA TRÊN KỸ THUẬT

-Signature là 1 bộ (mẫu) ngăn chặn tấn công đã đc biết trước ( chữ ký độc hai đã biết )

1. Kỹ thuật signature-based

-Signature-based IDS/IPS: Kỹ thuật này dựa trên các chữ ký hoặc tập luật của các cuộc tấn công đã biết trước để phát hiện các cuộc tấn công tương tự trong tương lai.

-Các chữ ký được cung cấp bởi các nhà sản xuất và được cập nhật thường xuyên. Kỹ thuật này rất hiệu quả trong việc phát hiện các cuộc tấn công đã biết trước, nhưng không thể phát hiện các cuộc tấn công mới hay sử dụng các kỹ thuật tấn công tiên tiến.

+ƯU :

- độ chính xác cao khi phát hiện tấn công đã biết , tỉ lệ sai thấp

+Nhược :

- không thê phát hiện nếu không biết trước

=> yêu cầu cập nhật liên tục CSDL

- Việc triển khai và cập nhật tốn tgian và khó

2.Anomaly-based Detection : định nghĩa bình thường , khác cái đó thì là bất thường

Profiles : đại diện cho hđ bình thường ( thông qua lịch sử lưu lượng mạng , các thống kê ML , clustering , fuzzy logic ,heuristic,… )

Anomaly-based IDS/IPS: Kỹ thuật này dựa trên phát hiện các hành vi bất thường trong hoạt động mạng hoặc hệ thống so với các mẫu hoạt động bình thường được xác định trước đó. Nó sử dụng các kỹ thuật học máy để học các mẫu hoạt động bình thường và cảnh báo khi có hành vi bất thường. Tuy nhiên, kỹ thuật này có thể phát hiện sai và cần một quá trình huấn luyện kỹ lưỡng để đảm bảo tính chính xác.

1. Specification-based : tập trung vào việc phát hiện các hoạt động không tuân thủ chính sách đã định sẵn

Specification-based sử dụng một mô tả chính xác về hành vi hợp lệ của một hệ thống để phát hiện các hành vi không hợp lệ hoặc tấn công. Điều này đòi hỏi các chuyên gia an ninh mạng phải có hiểu biết sâu về hệ thống và các phương thức tấn công để xác định các luật và chính sách bảo mật để bảo vệ hệ thống

Vd : request phải có http , domain ,url , …

Thiếu => cảnh báo lên

+ƯU:

* Xác định đc lệnh bất thường , ktra đc tính hợp lý của câu lệnh
* False positive thấp

+Nhược :

* Khó , thậm chỉ không thể phát triển các mô hình giao thức chính xác hoàn toàn

Hybrid :

+ƯU:

* Đối phó đc hành vi tinh vi trong tấn công
* Tích hợp 3 kỹ thuật cho trc
* Khắc phục nhiều nhược

+Nhược:

* Giới hạn phạm vi hoạt động của 1 chương trình giao thức
* Cần tích hợp cả 3 kỹ thuật riêng cho hđ trong cùng 1 hệ thống

1. DỰA TRÊN NGUỒN DỮ LIỆU
2. Network-based IDPS

* Theo dõi,phân tích hoạt động, lưu lượng mạng,giao thức thông qua sensor để xác định hành vi bất thường
* **Sự kiện trong mạng** là các hoạt động xảy ra trên mạng, bao gồm **các hoạt động như kết nối** và **ngắt kết nối, truyền dữ liệu, các giao thức mạng như TCP, UDP, ICMP** và các hoạt động tương tự. Những sự kiện này thường được ghi lại trong các log của thiết bị mạng như router, firewall hoặc IDS và được sử dụng để phát hiện các cuộc tấn công mạng, các lỗ hổng bảo mật hoặc các hoạt động xâm nhập mạng khác.

1. Host-based IDPS

* Theo dõi các sự kiện trong host
* **Sự kiện trong host** (hay còn gọi là sự kiện hệ thống) là các **hoạt động xảy ra trên máy tính** hoặc thiết bị đầu cuối (endpoints), bao gồm **các hoạt động hệ thống như khởi động, tắt, cài đặt phần mềm, truy cập file hệ thống, đăng nhập** và các hoạt động tương tự. Những sự kiện này thường được ghi lại trong các **file log** và được sử dụng để **phát hiện các hoạt động độc hại** như **malware** hoặc các **hành vi xâm nhập**.

1. Hybrid IDPS

* Kết hợp cả 2 cái trên

AGENT : HOST

SENSOR : NETWORK

Server quản lí : thu thập thông tin của sensor và agent

CÁC KHẢ NĂNG BẢO MẬT

1. Thu thập thông tin
2. Ghi log

* Tập trung , nội bộ

1. Phát hiện

A, ngưỡng

* Ngưỡng ( threshholds ) : giá trị thiết lập giới hạn
* Vd : 1p chỉ đc 100 request

B,Thiết lập cảnh báo

Triển khai

* Nắm rõ thiết kế
* Kiểm tra tp
* Bảo trì , cập nhật vá lỗi ,…