TCP/IP Stack

Tại sao phải chia tầng

* Không biết hết nổi

Đóng gói dữ liệu

**NIDPS : Kiến trức và vị trí của sensor**

**Inline sensor :**

* lưu lượng mạng đi qua ,
* cho phép ngăn chặn tấn công
* Các inline sensor thường được đặt gần đối tượng cần đo để có thể đo lường thông số vật lý hoặc hóa học của đối tượng đó một cách chính xác và liên tục. Vị trí đặt sensor cần đảm bảo tiếp cận được đối tượng cần đo, dễ dàng để bảo trì, sửa chữa và thay thế khi cần thiết.

**Passive sensor :**

* Theo dõi bản copy của lưu lượng mạng
* Không có lưu lượng thực tế đi qua
* Các passive sensor thường được đặt ở các vị trí đối diện hoặc xa hơn đối tượng cần đo. Vị trí đặt sensor phải đảm bảo tầm nhìn rõ ràng đến đối tượng cần giám sát, tránh những vật cản ảnh hưởng đến quá trình giám sát, và đảm bảo vị trí đặt an toàn và dễ dàng để bảo trì.

**Network TAPS (Terminal Access Point)**

* **Copy luu luong mang dua qua passive IDS**
* **Nếu TAP hư thì mất chức năng trên nhưng lưu lượng mạng vẫn đc đảm bảo**
* Fall-safe (hay còn gọi là fail-safe) là tính năng của một hệ thống, sản phẩm hoặc quy trình **được thiết kế** để **đảm bảo an toàn** hoặc **trở về trạng thái an toàn** khi xảy ra sự cố hoặc lỗi hệ thống.
* Trong một hệ thống fall-safe**, nếu có lỗi** xảy ra, hệ thống sẽ **tự động chuyển đến một trạng thái an toàn** hoặc ngừng hoạt động để tránh nguy hiểm cho người dùng hoặc hệ thống. Điều này giúp giảm thiểu nguy cơ tai nạn và giảm thiểu thiệt hại gây ra cho hệ thống hoặc sản phẩm.
* Ví dụ về fall-safe là hệ thống phanh trên ô tô. Nếu có lỗi xảy ra, chẳng hạn như mất áp suất phanh, hệ thống phanh fall-safe sẽ tự động kích hoạt để đảm bảo rằng xe dừng lại an toàn. Tương tự, các hệ thống điều khiển máy bay cũng được thiết kế với tính năng fall-safe để đảm bảo an toàn khi xảy ra sự cố.

**Switch port mirroring**

* Span port không bắt đc all lưu lượng khi config sai or quá tải
* **Port mirroring** là một tính năng trong mạng máy tính cho phép **sao chép lưu lượng truy cập** trên một cổng mạng (port) hoặc một nhóm cổng mạng và **gửi nó đến một cổng khác để phân tích và giám sát lưu lượng mạng.** Tính năng này còn được gọi là port monitoring, port sniffing hoặc port forwarding

**Phát hiện tấn công**

Sử dụng kq quét lỗ hổng để xác định tấn công

Hạn chế :

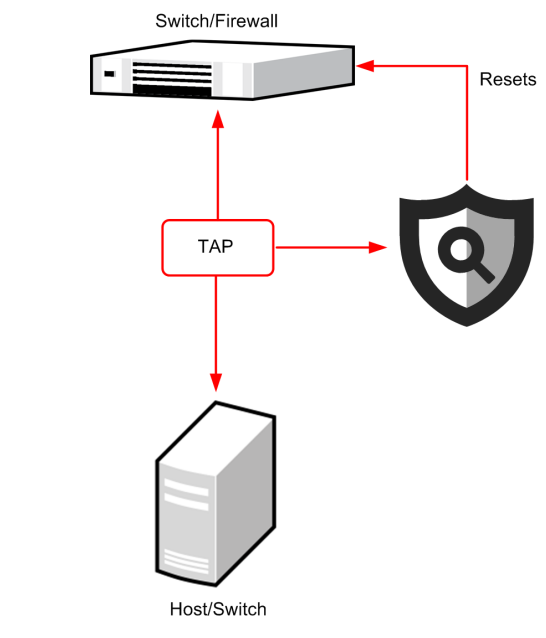
* Bị giới hạn hoặc không thể phân tích lưu lượng mạng đã mã hóa
* Xử lý tải lưu lượng cao
* Hứng chịu tấn công vào chính NIDPS

Passive mode :

* Vì phải phân tích bản sao lưu lượng nên có thể ngăn chặn chậm do gửi reset chậm hơn tấn công

2 con TAP hđ cùng lúc , đồng bộ dữ liệu

**IDS vs reset interface**

* Gửi cờ reset : ngắt session , tự động chặn tấn công (chỉ đc vs tcp , tấn công nhanh quá thì k chặn đc vì nó phải phân tích lưu lượng)
* 

**IPS trong inline mode**

**Diagram

Description automatically generated**

* Nội bộ tấn công nhau thì đi