**Nguyên lý hoạt động của hệ thống phát hiện xâm nhập mạng**

Giám sát mạng : thu thập thông tin lưu thông trên mạng thực hiện bằng các sensor.Yêu cầu đòi hỏi với giai đoạn này là có được thông tin đầy đủ và toàn vẹn về hình tình mạng

Phân tích lưu thông : khi đã thu thập được các thông tin cần thiết, IDS tiến hành phân tích dữ liệu thu thập được. Mỗi hệ thống cần có sự phân tích khác nhau vì không phải môi trường nào cũng giống nhau. Nếu phát hiện ra dấu hiệu tấn công các sensor sẽ gửi cảnh báo về cho trung tâm tổng hợp.

Liên lạc giữa các thành phần : việc liên lạc diễn ra khi các sensor phát hiện dấu hiệu tấn công, sử dụng bộ giao thức đặc biệt để trao đổi thông tin giữa các thành phần.Các giao thức này phải đảm bảo bí mật và chịu lỗi tốt.

Cảnh báo về các hành vi xâm nhập: sau khi phân tích xong dữ liệu, IDS đưa ra các cảnh báo như địa chỉ ko hợp lệ, ....

Tiến hành phản ứng lại: trong 1 số hệ thống ids không những cảnh báo cho người quản trị mà còn đưa ra các hành vi phòng vệ ngăn chặn hành vi tấn công đó. Các hành động IDS có thể đưa ra như : ngắt dịch vụ, cấm địa chỉ ip tấn công, tạo log,....

**Các phương pháp phát hiện bất thường**

**- Threshold Detection:** Kỹ thuật này nhấn mạnh thuật ngữ “đếm”. Các mức ngưỡng về  
các hoạt động bình thường được đặt ra, nếu có sự bất thường nào đó như login với số lần  
quá quy định, số lượng các tiến trình hoạt động trên CPU, số lượng một loại gói tin được  
gửi vượt quá mức. . .

**- Seft-learning Detection:** Kỹ thuật dò này bao gồm hai bước, khi thiết lập hệ thống  
phát hiện tấn công, nó sẽ chạy ở chế độ tự học và thiết lập một profile mạng với các hoạt  
động bình thường. Sau thời gian khởi tạo, hệ thống sẽ chạy ở chế độ sensor theo dõi các  
hoạt động bất thường của mạng so với profile đã thiết lập. Chế độ tự học có thể chạy song  
song với chế độ sensor để cập nhật bản profile của mình nhưng nếu dò ra có tín hiệu tấn  
công thì chế độ tự học phải dừng lại tới khi cuộc tấn công kết thúc.

**- Anomaly protocol detection:** Kỹ thuật dò này căn cứ vào hoạt động của các giao  
thức, các dịch vụ của hệ thống để tìm ra các gói tin không hợp lệ, các hoạt động bất thường  
là dấu hiệu của sự xâm nhập, tấn công. Kỹ thuật này rất hiệu quả trong việc ngăn chặn các  
hình thức quét mạng, quét cổng để thu thập thông tin của các hacker.

**Chức năng vai trò tường lửa**

**a.Chức năng:**

Trong ngành mạng máy tính, bức tường lửa (tiếng Anh: firewall) là rào chắn mà một  
số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng  
mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ  
bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

Tường lửa hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các tòa nhà.

Nhiệm vụ cơ bản của tường lửa là kiểm soát giao thông dữ liệu giữa hai vùng có độ  
tin cậy khác nhau. Các vùng tin cậy điển hình bao gồm: mạng Internet (vùng không đáng tin cậy) và mạng nội bộ (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc quyền tối thiểu.

**b. Vai trò**

Mạng internet ngày càng phát triển và phổ biến rộng khắp mọi nơi, lợi ích của nó rất  
lớn. Tuy nhiên cũng có rất nhiều ngoại tác không mong muốn đối với các cá nhân là cha mẹ hay tổ chức, doanh nghiệp, cơ quan nhà nước... như các trang web không phù hợp lứa tuổi, nhiệm vụ, lợi ích, đạo đức, pháp luật hoặc trao đổi thông tin bất lợi cho cá nhân, doanh  
nghiệp... Do vậy họ (các cá nhân, tổ chức, cơ quan và nhà nước) sử dụng tường lửa để ngăn  
chặn.  
Tường lửa đóng vai trò rất quan trọng để ngăn chặn các thành phần nguy hiểm như  
hacker, sâu, hay các loại virus trước khi chúng có thể xâm nhập vào máy tính của ta.

**Phân loại tường lửa**

Firewall cứng là những Firewall được tích hợp trên Router.

Đặc điểm của Firewall cứng:

• Không được linh hoạt như Firewall mềm: không thể thêm chức năng, thêm quy tắc như Firewall mềm.

• Firewall cứng hoạt động ở tầng thấp hơn Firewall mềm (tầng Network và tầng Transport)

• Firewall cứng không thể kiểm tra nội dung của một gói tin.

• Một số Firewall cứng thông dụng: NAT, Cisco ASA 5500,….

Firewall mềm là những Firewall được cài đặt trên các Server

Đặc điểm của Firewall mềm:

• Tính linh hoạt cao: có thể thêm, bớt các quy tắc, các chức năng.

• Firewall mềm hoạt động ở tầng cao hơn Firewall cứng (Tầng Applycation)

• Firewall mềm có thể kiểm tra được nội dung của gói tin (thông qua các từ khóa)

• Một số Firewall mềm thông dụng: Zone Alarm, Microsoft ISA Server 2006, Norton Firewall,….

**Virus máy tính, worm**

**Virus** là một loại mã độc có khả năng tự nhân bản và lây nhiễm chính nó vào các tệp hoặc chương trình máy tính. Virus phải luôn bám vào vật chủ để lây lan.

Đặc điểm của virus là nó có thể tự đính kèm vào một chương trình khác và thực thi bí mật khi chương trình mang virus kích hoạt. Khi virus được thực thi nó có thể làm bất kỳ việc gì trên hệ thống như thay đổi, sao chép hoặc xóa tệp chương trình.Vòng đời gồm 4 giai đoạn: Trú ẩn – Lây lan – Kích hoạt – Thực thi

Virus thường trú, tệp chương trình, đa hình, boot, macro, email.

**Worm** là chương trình độc hại có khả năng tự nhân bản và tự lây nhiễm trong hệ thống mà không cần tệp chủ để mang nó. Như vậy Worm không bám vào một tệp hoặc một vùng nào đó trên đĩa cứng.

Mục tiêu của worm là làm lãng phí băng thông của mạng, phá hoại hệ thống như xóa tệp, tạo ra backdoor cho phép kiểm soát máy tính nạn nhân. Sự tấn công của worm là cực kỳ nhanh chóng vì không cần tác động của con người.

Worm 2 loại: worm dịch vụ mạng lan truyền bằng các lỗ hổng bảo mật của mạng

Worm gửi thư hàng loạt tấn công qua dịch vụ thư điện tử

**Phương pháp phòng chống mã độc trong mạng**

**Luôn luôn cài đặt và sử dụng một phần mềm diệt virus chính hãng.** Ví dụ: Kaspersky, Bitdifender, Avast, Norton, Bkav...

**Cập nhật máy tính, phần mềm diệt virus**

Thực hiện quét virus định kỳ

- quét phần mềm độc hại trên các phương tiện thông tin từ bên ngoài trước khi sử dụng chúng.

- các tập tin đính kèm email phải được quét virus trước khi chúng được mở ra.

- Cấm gửi hoặc nhận một số loại tập tin giống như các tập tin .exe qua email.

- Hạn chế hoặc cấm sử dụng phần mềm không cần thiết

- Hạn chế việc sử dụng các phương tiện lưu trữ di động (các ổ đĩa flash…), đặc biệt là trên các máy chủ có nguy cơ lây nhiễm cao, các trạm truy cập mạng công cộng….

+ Không truy cập các trang web có thể chứa nội dung độc hại.

+ Không kích chuột vào trình duyệt web, cửa sổ popup nghi ngờ độc hại.

+ Không mở các tập tin với phần mở rộng như .Bat, .com, .exe, .pif, .vbs, thường có nhiều khả năng được liên kết với các phần mềm độc hại.

+ Không vô hiệu hóa các cơ chế kiểm soát an ninh, phần mềm độc hại (như phần mềm  chống virus, tường lửa cá nhân).

+ Không tải hoặc thực hiện các ứng dụng từ các nguồn không tin cậy.

+ Không bao giờ trả lời email yêu cầu thông tin tài chính hoặc cá nhân.

+ Chỉ nhập thông tin vào các trang web hoặc ứng dụng hợp pháp.