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

5 giai đoạn chính: Giám sát mạng, Phân tích lưu thông, Liên lạc giữa các thành phần, Cảnh báo về các hành vi xâm nhập, tiến hành Phản ứng lại tùy theo chức năng của từng IDS.

**• Giám sát mạng (Monotoring):** Giám sát mạng là quá trình thu thập thông tin về lưu  
thông trên mạng. Việc này thông thường được thực hiện bằng các Sensor. Yêu cầu  
đòi hỏi đối với giai đoạn này là có được thông tin đầy đủ và toàn vẹn về tình hình  
mạng.

**• Phân tích lưu thông (Analyzing):** Khi đã thu thập được những thông tin cần thiết từ  
những điểm trên mạng. IDS tiến hành phân tích những dữ liệu thu thập được. Mỗi hệ  
thống cần có một sự phân tích khác nhau vì không phải môi trường nào cũng giống  
nhau. Thông thường ở giai đoạn này, hệ thống IDS sẽ dò tìm trong dòng traffic mạng  
những dấu hiệu đáng nghi ngờ dựa trên kỹ thuật đối sánh mẫu hoặc phân tích hành vi  
bất thường. Nếu phát hiện ra dấu hiệu tấn công, các Sensor sẽ gửi cảnh báo về cho  
trung tâm để tổng hợp.

**• Liên lạc:** Giai đoạn này giữ một vai trò quan trọng trong hệ thống IDS. Việc liên lạc diễn ra khi Sensor phát hiện ra dấu hiệu tấn công hoặc Bộ xử lý thực hiên thay đổi cấu hình, điều khiển Sensor. Thông thường các hệ thống IDS sử dụng các bộ giao thức đặc biệt để trao đổi thông tin giữa các thành phần. Các giao thức này phải đảm bảo tính Tin cậy, Bí mật và Chịu lỗi tốt, ví dụ: SSH, HTTPS, SNMPv3 . . .Chẳng hạn hệ thống IDS của hãng Cisco thường sử dụng giao thức PostOffice định nghĩa một tập các Thông điệp để giao tiếp giữa các thành phần.

**• Cảnh báo (Alert):** Sau khi đã phân tích xong dữ liệu, hệ thống IDS cần phải đưa ra được  
những cảnh báo. Ví dụ như:

- Cảnh báo địa chỉ không hợp lệ.

- Cảnh báo khi một máy sử dụng hoặc cố gắng sử dụng những dịch vụ không hợp lệ.  
- Cảnh báo khi máy cố gắng kết nối đến những máy nằm trong danh sách cần theo dõi ở trong hay ngoài mạng.

**• Phản ứng (Response):** Trong một số hệ thống IDS tiên tiến hiện nay, sau khi các giai đoạn trên phát hiện được dấu hiệu tấn công, hệ thống không những cảnh báo cho người quản trị mà còn đưa ra các hành vi phòng vệ ngăn chặn hành vi tấn công đó. Điều này giúp tăng cường khả năng tự vệ của Mạng, vì nếu chỉ cần cảnh báo cho người quản trị thì đôi khi cuộc tấn công sẽ tiếp tục xảy ra gây ra các tác hại xấu. Một hệ thống IDS có thể phản ứng lại trước những tấn công phải được cấu hình để có quyền can thiệp vào hoạt động của Firewall, Switch và Router. Các hành động mà IDS có thể đưa ra như:

- Ngắt dịch vụ.

- Gián đoạn phiên.

- Cấm địa chỉ IP tấn công.

- Tạo log.

**2. Các phương pháp phát hiện bất thường**

**- Xác xuất thống kê** : được sử dụng nhiều trong các hệ thống phát hiện bất thường. Phương pháp này sử dụng mô hình xác xuất để mô tả tất cả các hoạt động trong hệ thống mạng. Mục tiêu của phương pháp này là thiết lập một mô hình dữ liệu phù hợp để lưu trữ tri thức về tính bình thường của lưu thông mạng, dựa vào đó có thể đánh giá được tính bất thường tại từng thời điểm cụ thể. Trong phương pháp này, hệ thống quan sát hành vi của các đối tượng và lập profile về tập hành vi đó. Profile thông thường bao gồm các đại lượng đo lường về mật độ, cường độ hoạt động, đo lường theo từng loại hoạt động, các thông số kỹ thuật như CPU, Ram ... Một số hệ thống: haystack, spade, nides

- **Máy trạng thái hữu hạn:** người ta có thể dùng mô hình máy trạng thái hữu hạn FSM (Finite State Machine) để giải quyết bài toán phát hiện BTTM. Theo hướng này, các FSM sẽ xây dựng chuỗi các hành vi diễn ra trong trạng thái hoạt động bình thường, từ đó phát hiện ra quá trình xuất hiện lỗi. Dựa trên các số liệu đã được ghi lại trước đó, người ta sẽ xây dựng được mô hình FSM theo xác suất về các sự cố trên mạng. Từ đó, FSM không chỉ tập trung vào việc phát hiện ra các sự cố mạng mà còn giải quyết được bài toán xác định nguyên nhân dẫn đến sự cố. Các chuỗi báo động ở các điểm khác nhau trên mạng sẽ được ghi nhận thành trạng thái của máy.

**- Phát hiện bất thường bằng mạng Nơ-ron:** hệ thống IDS sử dụng mạng Nơ-ron thường là host-based IDS, tập trung vào việc phát hiện các thay đổi trong hành vi của chương trình như là dấu hiệu bất thường. Theo cách tiếp cận này, mạng Nơ-ron sẽ học và dự đoán hành vi của người sử dụng và các chương trình tương ứng. Ưu điểm của mạng Nơ-ron là dễ dàng thích ứng với các kiểu dữ liệu không đầy đủ, dữ liệu với độ chắc chắn không cao, đồng thời phương pháp này cũng có khả năng đưa ra các kết luận mà không cần cập nhật tri thức thường xuyên. Điểm yếu của mạng Nơ-ron là tốc độ xử lý do hệ thống cần thu thập dữ liệu, phân tích và điều chỉnh từng Nơ-ron để cho kết quả chính xác. Một số hệ thống IDS điển hình như : IDS sử dụng mạng Nơ-ron lan truyền ngược hay mạng Nơ-ron hồi quy

**- Phát hiện bất thường bằng hệ chuyên gia:** phương pháp này có tên gọi là Rule based detection (phát hiện trên tập luật). Đây là một trong những hướng tiếp cận đầu tiên để giải quyết vấn đề phát hiện bất thường trong mạng. Phương pháp rule based dựa trên hệ chuyên gia, cần có một CSDL đồ sộ bao gồm các luật để mô tả hành vi bất thường để phát hiện lỗi trên hệ thống. Các hệ thống rule based này trong thực tế không được sử dụng nhiều do hệ thống chạy quá chậm không thể đáp ứng được thời gian thực, đồng thời cần phải có trước tri thức về tình trạng của các cuộc tấn công như: mạng quá tải, số lượng kết nối TCP nhiều bất thường,... Phụ thuộc lớn vào kinh nghiệm của người quản trị.

- **Phát hiện bất thường bằng khai phá dữ liệu:** so với kỹ thuật khác có ưu thế rõ rệt, KPDL có thể sử dụng với các CSDL chứa nhiều nhiễu, dữ liệu không đầy đủ hoặc biến đổi liên tục, mức độ sử dụng chuyên gia ko quá thường xuyên. Dựa trên các ưu thế đó, KPDL cũng đc các nhà nghiên cứu áp dụng vào hệ thống phát hiện xâm nhập trái phép. Khả năng xử lý khối lượng dữ liệu lớn. Có 2 hướng chính phát hiện trên hành vi lạm dụng và bất thường.

**3. Chức năng và vai trò của tường lửa.**

**a.Chức năng:**

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 ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

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 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, worm, hay các loại virus trước khi chúng có thể xâm nhập vào máy tính của ta.

**4. Phân loại tường lửa:**

**Có ba loại tường lửa cơ bản tùy theo:**

- Truyền thông được thực hiện giữa một nút đơn và mạng, hay giữa một số mạng:

* Tường lửa cá nhân hay tường lửa máy tính, một ứng dụng phần mềm với chức năng

thông thường là lọc dữ liệu ra vào một máy tính đơn.

* Tường lửa mạng thường chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các khu phi quân sự.

- Truyền thông được chặn tại tầng mạng hay tại tầng ứng dụng:

* Tường lửa tầng mạng. Ví dụ iptables.
* Tường lửa tầng ứng dụng. Ví dụ TCP Wrappers.
* Tường lửa ứng dụng. Ví dụ: hạn chế các dịch vụ ftp bằng việc định cấu hình tại tệp

/etc/ftpaccess.

- Tường lửa có theo dõi trạng thái của truyền thông hay không:

* Tường lửa có trạng thái (Stateful firewall)
* Tường lửa phi trạng thái (Stateless firewall)

**5. Virus máy tính, Worm**

**a. Virus:**

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, mail.

***- Phân loại Virus.***

Một trong những phương pháp thường thấy để phân loại virus là theo cách lây nhiễm của  
chúng. Phương pháp này chia virus ra làm 3 loại: Virus lây nhiễm boot-sector, virus lây  
nhiễm các file thực thi và virus lây nhiễm các file dữ liệu.

**b.Worm:**

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.

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

Sâu máy tính thường mang theo phần mềm gián điệp để mở cửa hậu máy tính trên  
các máy tính bị nhiễm (giống như Sobig và Mydoom). Các máy tính bị nhiễm được sử dụng bởi những người gửi thư rác hoặc giả danh địa chỉ trang web. Các cửa hậu cũng có thể được các sâu máy tính khác khai thác như Doomjuice - phát tán bằng cửa hậu được mở bởi Mydoom.

Sâu máy tính lan truyền qua mạng hay qua các thiết bị lưu trữ di động như USB.

**6. Phương pháp phòng chống mã độc qua mạng**

a. Sử dụng phần mềm diệt virus

b. Sử dụng tường lửa

c. Cập nhận các bản sửa lỗi của hệ điều hành

d. Vận dụng kinh nghiệm sử dụng máy tính

- Phát hiện sự hoạt động khác thường của máy tính

- Kiểm soát các ứng dụng đang hoạt động

- Loại bỏ một số tính năng của hệ điều hành có thể tạo điều kiện cho sự lây nhiễm mã độc.

e. Bảo vệ dữ liệu máy tính

**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.