**TƯỜNG LỬA, HỆ THỐNG PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP.**

1. **Tường lửa là gì? Đặc điểm của tưởng lửa và các chính sách truy cập.**
   1. **Khái niệm**

Tường lửa (firewall) là một phần mềm hoặc phần cứng được sử dụng để kiểm soát luồng thông tin giữa các mạng hoặc giữa một mạng và internet. Chức năng chính của tường lửa là bảo vệ mạng máy tính khỏi các cuộc tấn công từ bên ngoài và kiểm soát quyền truy cập vào các tài nguyên mạng từ bên trong mạng.

* 1. **Đặc điểm**

**Kiểm soát truy cập:** Tường lửa có thể cấu hình để cho phép hoặc từ chối các kết nối từ hoặc đến các địa chỉ IP, cổng và giao thức cụ thể. Điều này giúp ngăn chặn các cuộc tấn công từ bên ngoài và kiểm soát quyền truy cập vào tài nguyên mạng từ bên trong mạng.

**Quản lý luồng dữ liệu:** Tường lửa có thể kiểm soát luồng dữ liệu đi qua mạng dựa trên các quy tắc được cấu hình trước. Điều này cho phép tường lửa phân loại và kiểm soát dữ liệu dựa trên loại, nguồn, đích và nhiều yếu tố khác.

**Bảo vệ chống tấn công:** Tường lửa có thể phát hiện và ngăn chặn các cuộc tấn công mạng như tấn công từ chối dịch vụ (DoS), tấn công dò lỗ hổng (port scanning), và các hình thức tấn công khác.

**Ghi nhật ký (Logging):** Tường lửa có thể ghi lại các sự kiện mạng quan trọng như các yêu cầu truy cập bị từ chối, cố gắng tấn công và các hoạt động mạng khác để phục vụ cho mục đích giám sát, phân tích và điều tra.

* 1. **Chính sách truy cập**

Chính sách truy cập tường lửa là tập hợp các quy tắc và nguyên tắc được cấu hình trên tường lửa để quản lý và kiểm soát quyền truy cập vào mạng. Các chính sách này có thể xác định các quy tắc cho phép hoặc từ chối truy cập dựa trên địa chỉ IP, cổng, giao thức, ứng dụng, người dùng, hoặc các yếu tố khác. Chính sách truy cập được thiết lập để đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào tài nguyên mạng cần thiết và để ngăn chặn các cuộc tấn công từ bên ngoài.

1. **Phân loại tường lửa.**

**Theo cách hoạt động:**

Tường lửa gói: Kiểm soát luồng dữ liệu dựa trên thông tin trong các gói dữ liệu, bao gồm địa chỉ IP nguồn và đích, số cổng và giao thức.

Tường lửa ứng dụng: Kiểm soát dựa trên dữ liệu ứng dụng, có thể phân biệt các ứng dụng cụ thể như HTTP, FTP, SMTP, v.v.

**Theo vị trí triển khai:**

Tường lửa mạng (Network firewall): Triển khai ở cổng ra vào giữa mạng nội bộ và internet hoặc mạng ngoại vi khác.

Tường lửa máy tính (Host firewall): Triển khai trên một máy tính cụ thể để bảo vệ chính máy tính đó.

Theo mức độ phức tạp:

Tường lửa cơ bản (Basic firewall): Cung cấp các tính năng cơ bản như kiểm soát truy cập dựa trên địa chỉ IP và cổng.

Tường lửa tiên tiến (Advanced firewall): Bao gồm các tính năng nâng cao như phân tích dữ liệu ứng dụng, phát hiện và ngăn chặn các mối đe dọa mạng phức tạp.

**Theo mục đích sử dụng:**

Tường lửa thông qua chính sách (Policy-based firewall): Áp dụng các chính sách cụ thể để quyết định liệu một kết nối được cho phép hay bị từ chối dựa trên các yếu tố như địa chỉ IP, cổng và giao thức.

Tường lửa dựa trên trạng thái (Stateful firewall): Theo dõi trạng thái của các kết nối mạng và quyết định liệu gói dữ liệu đến có phải là một phản hồi hợp lệ cho một yêu cầu trước đó hay không.

1. **Các nền tảng tường lửa.**

Cisco ASA (Adaptive Security Appliance): Cisco ASA là một trong những nền tảng tường lửa hàng đầu, được sử dụng rộng rãi trong doanh nghiệp và tổ chức. Nó cung cấp các tính năng bảo mật mạng toàn diện bao gồm tường lửa, VPN, IPS (Intrusion Prevention System), và nhiều tính năng khác.

Palo Alto Networks: Palo Alto Networks cung cấp các nền tảng tường lửa dựa trên phần cứng và phần mềm như Palo Alto Networks Next-Generation Firewall (NGFW). Các sản phẩm của Palo Alto Networks nổi tiếng với khả năng phát hiện và ngăn chặn các mối đe dọa mạng cũng như cung cấp quản lý bảo mật toàn diện.

Fortinet FortiGate: FortiGate là một loạt các thiết bị tường lửa do Fortinet cung cấp, bao gồm cả phần cứng và phần mềm. FortiGate tích hợp nhiều tính năng bảo mật như tường lửa, IPS, VPN, quản lý băng thông, và các tính năng khác trong một thiết bị duy nhất.

Check Point Firewall: Check Point là một nhà cung cấp hàng đầu về các giải pháp bảo mật mạng, bao gồm tường lửa, VPN, IPS, và các tính năng khác. Check Point Firewall cung cấp khả năng bảo vệ mạng khỏi các mối đe dọa mạng hiện đại và quản lý bảo mật hiệu quả.

pfSense: pfSense là một phần mềm tường lửa mã nguồn mở dựa trên hệ điều hành FreeBSD. Nó cung cấp một loạt các tính năng bảo mật mạnh mẽ và linh hoạt như tường lửa, VPN, DHCP, DNS, và nhiều tính năng khác.

OpenWrt: OpenWrt là một hệ điều hành mã nguồn mở được sử dụng chủ yếu cho các thiết bị mạng như router và access point. Nó cung cấp các tính năng tường lửa cơ bản cùng với khả năng tùy chỉnh và mở rộng.

1. **Phát hiện xâm nhập( Nguyên tắc cơ bản, Sự sai lầm tỉ lệ cơ sở, Yêu cầu ).**
   1. **Nguyên tắt cơ bản**

Nguyên tắc chính xác: Hệ thống phát hiện xâm nhập cần có khả năng phân biệt giữa các hoạt động hợp lệ và không hợp lệ một cách chính xác. Sự nhầm lẫn có thể dẫn đến các cảnh báo không chính xác hoặc bỏ qua các mối đe dọa thực sự.

Nguyên tắc toàn vẹn và bảo mật: Hệ thống phát hiện xâm nhập cần đảm bảo rằng dữ liệu được thu thập và xử lý một cách an toàn và không bị thay đổi, giả mạo hoặc tiết lộ cho bên thứ ba không mong muốn.

Nguyên tắc hiệu suất: Hệ thống phát hiện xâm nhập cần có hiệu suất cao để có thể phát hiện và phản ứng đối với các mối đe dọa một cách nhanh chóng và chính xác.

Nguyên tắc linh hoạt và mở rộng: Hệ thống phát hiện xâm nhập cần có khả năng linh hoạt và mở rộng để có thể thích ứng với các môi trường mạng đang phát triển và các mối đe dọa mới.

* 1. **Sai lầm tỉ lệ cơ sở**

Sự sai lầm tỉ lệ cơ sở (Baseline Error Rate) là tỷ lệ số lần hệ thống phát hiện xâm nhập báo cáo về các sự kiện không hợp lệ mà thực tế là hợp lệ. Sự sai lầm tỉ lệ cơ sở càng thấp càng tốt, vì nó đảm bảo rằng hệ thống chỉ tạo ra các cảnh báo khi thực sự có mối đe dọa.

* 1. **Yêu cầu**

Thu thập dữ liệu: Hệ thống phát hiện xâm nhập cần thu thập dữ liệu từ nhiều nguồn khác nhau trên mạng và hệ thống để phát hiện các mô hình hoạt động không bình thường.

Phân tích và xử lý dữ liệu: Dữ liệu thu thập được cần được phân tích và xử lý để phát hiện ra các hoạt động không hợp lệ và mối đe dọa potenial.

Xác định và phản ứng: Hệ thống cần xác định các sự kiện đáng ngờ và phản ứng thông qua việc tạo ra cảnh báo hoặc thực hiện các biện pháp an ninh phù hợp để đối phó với mối đe dọa.

Giám sát và điều chỉnh: Hệ thống phát hiện xâm nhập cần được liên tục giám sát và điều chỉnh để đảm bảo rằng nó có khả năng phát hiện các mối đe dọa mới và thích ứng với các biến đổi trong môi trường mạng.

1. **Phát hiện Xâm nhập dựa trên Host (Khả năng phát hiện cục bộ), Phát hiện Xâm nhập dựa trên môi trường Mạng (Khả năng phát hiện dựa trên kết nối)**
   1. **Phát hiện xâm nhập dựa trên Host**

Phát hiện xâm nhập dựa trên host tập trung vào việc giám sát và phân tích các hoạt động trên từng máy chủ hoặc thiết bị mạng cụ thể.

Các hệ thống phát hiện xâm nhập dựa trên host thường được triển khai trực tiếp trên các máy chủ hoặc thiết bị, và chúng kiểm tra các log, tệp tin hệ thống, và các hoạt động của các tiến trình và dịch vụ cục bộ.

Các kỹ thuật phát hiện xâm nhập dựa trên host thường sử dụng các mẫu hoặc quy tắc để xác định các mô hình hoạt động không bình thường hoặc có hại trên mỗi máy chủ.

* 1. **Phát hiện xâm nhập dựa trên môi trường mạng.**

Phát hiện xâm nhập dựa trên môi trường mạng tập trung vào việc giám sát và phân tích các hoạt động trên mạng trong khi chúng diễn ra qua các kết nối mạng.

Các hệ thống phát hiện xâm nhập dựa trên môi trường mạng thường được triển khai tại các điểm truy cập vào mạng hoặc trên các thiết bị chuyển mạch và định tuyến.

Chúng kiểm tra dữ liệu gói tin trên mạng để phát hiện ra các mô hình hoạt động không bình thường hoặc các dạng tấn công mạng như các gói tin độc hại hoặc dữ liệu phản hồi từ mạng ngoài.