**CHƯƠNG 1. TỔNG QUAN VỀ TẤN CÔNG VÀ PHÁT HIỆN TẤN CÔNG MẠNG**

#### **1.1. Tấn công trong mạng máy tính**

##### 1.1.1. Khái niệm về tấn công mạng

Tấn công mạng là hoạt động có chủ ý của kẻ phạm tội lợi dụng các lỗ hổng của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hê ̣thống thông tin.

##### 1.1.2. An toàn mạng

Internet ngày càng phát triển rộng rãi, vấn đề an ninh trên môi trường mạng ngày càng trở nên cấp thiết. Các cuộc tấn công mạng đang gia tăng cả về số lượng và mức độ nghiêm trọng. Các phương thức và hệ thống bảo mật truyền thống đã không còn hiệu quả để đảm bảo an toàn thông tin và dữ liệu cho các tổ chức, cá nhân. Yêu cầu cần có những giải pháp, công cụ tiên tiến hơn để bảo vệ thông tin và dữ liệu trên mạng máy tính.

An toàn mạng có thể hiểu là cách bảo vệ nhằm đảm bảo an toàn cho tất cả các thành phần của mạng bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng và đảm bảo mọi tài nguyên mạng được sử dụng tương ứng với một chính sách hoạt động được ấn định và với chỉ những người có thẩm quyền tương ứng.

An toàn mạng thường bao gồm: Xác định chính xác các khả năng, nguy cơ xâm nhập mạng, các sự cố rủi ro đối với thiết bị, dữ liệu trên mạng để có các giải pháp phù hợp đảm bảo an toàn mạng.

- Các kiểu vi phạm an toàn mạng

Các lỗ hổng về an toàn và bảo mật của hệ thống là những tình huống có khả năng gây mất mát và tổn hại hệ thống. Có 4 hiểm họa đối với an toàn hệ thống là: Sự phá hoại, sự sửa đổi, sự can thiệp và sự giả mạo.

+ Sự phá hoại: Tài nguyên của hệ thống sẽ bị mất đi, không ở trạng thái sẵn sàng hoặc không thể sử dụng được. Cố ý phá hoại các thiết bị phần cứng, xóa bỏ file dữ liệu, chương trình hoặc làm sai chức năng quản lý của hệ điều hành để nó không thể tìm ra được file cụ thể trên đĩa ...

+ Sự can thiệp: đối tượng không được phép có thể truy cập vào hệ thống sử dụng tài nguyên hệ thống hoặc sao chép chương trình, sao chép dữ liệu trái phép.

+ Sự sửa đổi: Thay đổi giá trị cơ sở dữ liệu, sửa đổi chương trình làm chương trình không hoạt động đúng với chức năng được thiết kế, thay đổi dữ liệu đang truyền

qua phương tiện điện tử.

+ Sự giả mạo: Giả mạo những đối tượng hợp pháp trong hệ thống, đưa ra giao dịch giả vào mạng truyền thông, thêm dữ liệu vào cơ sở dữ liệu hiện có.

- Các mục tiêu an toàn mạng

Đảm bảo an toàn mạng là nhằm mục đích đảm bảo cho tính đúng đắn, độ tin cậy cao nhất của thông tin được xử lý, đồng thời bảo vệ được các thông tin được lưu trữ trong các cơ sở dữ liệu và thông tin lưu chuyển trên mạng. Một hệ thống được xem là an toàn chỉ có sự kết hợp của ba đặc tính: Tính bảo mật, tính toàn vẹn và tính sẵn sàng của tài nguyên mạng và các dịch vụ mạng. Vấn đề an toàn thông tin còn thể hiện qua mối quan hệ giữa người sử dụng với hệ thống mạng và tài nguyên mạng. Các quan hệ này được đảm bảo bằng các phương thức xác thực, cấp phép sử dụng và từ chối phục vụ [1].

+ Tính bí mật: Thông tin phải đảm bảo tính bí mật và được sử dụng đúng đối tượng.

+ Tính toàn vẹn: Thông tin phải đảm bảo đầy đủ, nguyên vẹn về cấu trúc.

+ Tính sẵn sàng: Thông tin phải luôn sãn sàng để tiếp cận, phục vụ theo đúng mục đích và đúng cách.

+ Tính chính xác: Thông tin phải có độ chính xác và tin cậy.

+ Tính không khước từ: Thông tin có thể kiểm chứng được nguồn gốc hoặc người đưa tin.

##### 1.1.3. Lỗ hổng bảo mật

Lỗ hổng bảo mật là những lỗi phần mềm, lỗi trong đặc điểm kỹ thuật và thiết kế, nhưng đa số là lỗi trong lập trình. Cấu trúc phần mềm được thiết kế bởi con người, và những dòng code trong đó cũng được viết bởi con người, vì vậy việc xuất hiện lỗi là không thể tránh khỏi. Đây là những lỗ hổng nằm ủ mình trong hệ thống phần mềm, đợi đến khi bị phát hiện. Khi đó, chúng có thể được dùng để tấn công vào hệ thống. Các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ở các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows, UNIX; hoặc trong các ứng dụng mà người sử dụng thương xuyên sử dụng [1].

Phân loại lỗ hổng bảo mật :

* Lỗ hổng loại C: Các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo Dos. Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống.Không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.
* Lổ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình; Những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến mất hoặc lộ thông tin yêu cầu bảo mật.
* Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài có thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.  **1.1.4. Các kiểu tấn công mạng phổ biến**
* Tấn công thăm dò

Kiểu tấn công thăm dò là việc thu thập dữ liệu trái phép về tài nguyên, các lỗ hổng hoặc dịch vụ của hệ thống. Việc thăm dò được thăm dò theo các bước thăm dò thụ động (thu thập các thông tin được công khai) và thăm dò chủ động(sử dụng các công cụ để tìm kiếm thông tin trên máy tính của nạn nhân). Thăm dò nó cũng là một giai đoạn tấn công, trong giai đoạn này mục đích của người tấn công là thu thập mọi thông tin của hệ thống, tìm kiếm các lỗ hổng để thực hiện các giai đoạn tấn công tiếp theo.

* Nghe trộm (Eavesdropping)

Nhìn chung, phần lớn các thông tin liên lạc mạng diễn ra ở dạng rõ (cleartext) - định dạng không bảo đảm an toàn, cho phép kẻ tấn công có thể can thiệp vào dữ liệu trên mạng như nghe lén, chỉnh sửa nội dung thông tin... Nếu không có các dịch vụ mã hóa mạnh mẽ dựa trên mật mã, dữ liệu trên mạng có thể bị đọc bởi những kẻ có ý đồ xấu và gây ra tổn thất lớn cho cá nhân cũng như các tổ chức.

Việc nghe trộm thông tin trên đường truyền có thể được thực hiện bằng việc cài keylog, phần mềm chặn bắt gói tin, phân tích giao thức hay thậm chí là các thiết bị phần cứng hỗ trợ việc “lắng nghe” các thông tin liên lạc trên mạng.

* Tấn công truy cập

Tấn công truy cập là kiểu tấn công giúp người xâm nhập lấy được quyền truy cập trái phép của một hệ thống bảo mật với mục đích thao túng dữ liệu, nâng cao đặc quyền hay đơn giản chỉ là truy cập vào hệ thống.

+ Tấn công truy cập hệ thống: Người tấn công thường tìm kiếm quyền truy cập đến một thiết bị bằng cách chạy một đoạn mã, bằng những công cụ hỗ tợ (Hacking tool) hoặc là khai thác một điểm yếu của ứng dụng hay một dịch vụ đang chạy trên máy chủ.

+ Tấn công truy cập thao túng dữ liệu: Thao túng dữ liệu xuất hiện khi kẻ xâm nhập đọc, viết, xóa, sao chép hay thay đổi dữ liệu.

+ Tấn công truy cập nâng cao đặc quyền: Nâng cao đặc quyền là một dạng tấn công phổ biến. Bằng cách nâng cao đặc quyền, kẻ xâm nhập có thể truy cập vào các files hay folder dữ liệu mà tài khoản người sử dụng ban đầu không được cho phép truy cập. Khi kẻ xâm nhập đạt được mức độ quyền truy cập đủ cao, họ có thể cài đặt phần mềm như là backdoors và Trojan horses, cũng như cho phép truy cập sâu hơn và thăm dò. Mục đích chung là chiếm được quyền truy cập ở mức độ quản trị. Khi đã đạt được mục đích đó, họ có toàn quyền điều khiển hệ thống mạng.

- Tấn công từ chối dịch vụ

Đây là cách tấn công làm cho hệ thống bị tấn công quá tải không thể cung cấp dịch vụ, làm gián đoạn hoạt động của hệ thống hoặc hệ thống phải nhưng hoạt động.

Tùy theo phương thức thực hiện mà mà nó được biết dưới nhiều tên gọi khác nhau. Mục đích là lợi dụng sự yếu kém của giao thức TCP (Transmision control protocol) để thực hiện tấn công tưg chối dịch vụ Dos (Denial of Service), mới hơn là tấn công từ chối dịch vụ phân tán Ddos, mới nhất là tấn công từ chối dịch vụ theo phương pháp phản xạ Drdos.

+ Tấn công từ chối dịch vụ cổ điển

Tấn công từ chối dịch vụ cổ điển DoS là một phương pháp tấn công từ chối dịch vụ xuất hiện đầu tiên với các kiểu tấn công như Smurf Attack, Tear Drop, SYN Attack… Các kiểu tấn công này thường được áp dụng đối với đối tượng tấn công là hệ thống máy chủ bảo mật kém, băng thông (bandwidth) yếu, thậm chí trong nhiều trường hợp, đối tượng tin tặc có thể sử dụng đường truyền có tốc độ vừa phải cũng có thể thực hiện thành công các kiểu tấn công này.

Tear drop: Tất cả các dữ liệu chuyển đi trên mạng từ hệ thống nguồn đến hệ thống đích đều phải trải qua 2 quá trình: dữ liệu sẽ được chia ra thành các mảnh nhỏ ở hệ thống nguồn, mỗi mảnh đều phải có một giá trị offset định để xác định vị trí của mảnh đó trong gói dữ liệu được chuyển đi. Khi các mảnh này đến hệ thống đích, hệ thống đích sẽ dựa vào giá trị offset để sắp xếp các mảnh lại với nhau theo thứ tự đúng như ban đầu. Lợi dụng sơ hở đó, ta chỉ cần gởi đến hệ thống đích một loạt gói packets với giá trị offset chồng chéo lên nhau. Hệ thống đích sẽ không thể nào sắp xếp lại các packets này, nó không điều khiển được và có thể bị crash, reboot hoặc ngừng hoạt động nếu số lượng gói packets với giá trị offset chồng chéo lên nhau quá lớn.

SYN Attack: Trong SYN Attack, hacker sẽ gởi đến hệ thống đích một loạt SYN packets với địa chỉ ip nguồn không có thực. Hệ thống đích khi nhận được các SYN packets này sẽ gởi trở lại các địa chỉ không có thực đó và chờ đợi để nhận thông tin phản hồi từ các địa chỉ ip giả . Vì đây là các địa chỉ IP không có thực, nên hệ thống đích sẽ sẽ chờ đợi vô ích và còn đưa các “request” chờ đợi này vào bộ nhớ, gây lãng phí một lượng đáng kể bộ nhớ trên máy chủ mà đúng ra là phải dùng vào việc khác thay cho phải chờ đợi thông tin phản hồi không có thực này . Nếu ta gởi cùng một lúc nhiều gói tin có địa chỉ IP giả như vậy thì hệ thống sẽ bị quá tải dẫn đến bị crash hoặc boot máy tính.

Smurf Attack: Trong Smurf Attack, hacker sẽ gởi các gói tin ICMP đến địa chỉ broadcast của mạng khuếch đại. Điều đặc biệt là các gói tin ICMP packets này có địa chỉ ip nguồn chính là địa chỉ IP của nạn nhân. Khi các packets đó đến được địa chỉ broadcast của mạng khuếch đại, các máy tính trong mạng khuếch đại sẽ tưởng rằng máy tính nạn nhân đã gởi gói tin ICMP packets đến và chúng sẽ đồng loạt gởi trả lại hệ thống nạn nhân các gói tin phản hồi ICMP packets. Hệ thống máy nạn nhân sẽ không chịu nổi một khối lượng khổng lồ các gói tin này và nhanh chóng bị ngừng hoạt động, crash hoặc reboot.

UDP Flooding: Cách tấn công UDP đòi hỏi phải có 2 hệ thống máy cùng tham gia. Hackers sẽ làm cho hệ thống của mình đi vào một vòng lặp trao đổi các dữ liệu qua giao thức UDP. Và giả mạo địa chỉ IP của các gói tin là địa chỉ loopback (127.0.0.1) , rồi gởi gói tin này đến hệ thống của nạn nhân trên cổng UDP echo (7). Hệ thống của nạn nhân sẽ trả lời lại các messages do 127.0.0.1 (chính nó) gửi đến, kết quả là nó sẽ đi vòng một vòng lặp vô tận. Tuy nhiên, có nhiều hệ thống không cho dùng địa chỉ loopback nên hacker sẽ giả mạo một địa chỉ IP của một máy tính nào đó trên mạng nạn nhân và tiến hành ngập lụt UDP trên hệ thống của nạn nhân. Tấn công DNS: Hacker có thể đổi một lối vào trên Domain Name Server của hệ thống nạn nhân rồi cho chỉ đến một website nào đó của hacker. Khi máy khách yêu cầu DNS phân tích địa chỉ bị xâm nhập thành địa chỉ IP, lập tức DNS (đã bị hacker thay đổi cache tạm thời) sẽ đổi thành địa chỉ IP mà hacker đã cho chỉ đến đó. Kết quả là thay vì phải vào trang Web muốn vào thì các nạn nhân sẽ vào trang Web do chính hacker tạo ra. Một cách tấn công từ chối dịch vụ thật hữu hiệu.

+ Tấn công từ chối dịch vụ phân tán DDos:

Tấn công từ chối dịch vụ phân tán DDoS, so với tấn công DoS cổ điển, sức mạnh tăng gấp nhiều lần. Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống, dẫn đến ngưng hoạt động hệ thống. Để thực hiện DDoS, người tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính/mạng máy tính trung gian được gọi là botnet từ nhiều nơi để đồng loạt gửi ào ạt các gói tin với số lượng rất lớn nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó.

+ Tấn công từ chối dịch vụ phản xạ nhiều vùng DRDoS:

Tấn công từ chối dịch vụ phản xạ nhiều vùng DRDoS lại là kiểu tấn công mới nhất, mạnh nhất trong các kiểu tấn công DoS. Trong suốt quá trình máy chủ bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy chủ đó.

Tất cả các dịch vụ chạy trên nền TCP/IP như DNS, HTTP, FTP, POP3... đều bị vô hiệu hóa. Về cơ bản, DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS. Nó có kiểu tấn công SYN với một máy tính đơn, vừa có sự kết hợp giữa nhiều máy tính để chiếm dụng băng thông như kiểu DDoS. Kẻ tấn công thực hiện bằng cách giả mạo địa chỉ của máy chủ mục tiêu rồi gửi yêu cầu SYN đến các máy chủ lớn như Yahoo,

Microsoft, Google... để các máy chủ này gửi các gói tin SYN/ACK đến máy chủ mục tiêu. Quá trình cứ lặp lại liên tục với nhiều máy chủ lớn tham gia nên máy chủ mục tiêu nhanh chóng bị quá tải, băng thông (bandwitch) bị chiếm dụng bởi máy chủ lớn, dẫn đến máy chủ mục tiêu không thể hoạt động bình thường.

- Giả mạo (Spoofing)

Hầu hết các mạng và hệ điều hành sử dụng địa chỉ IP để xác nhận một đối tượng là hợp lệ. Trong một số trường hợp, một địa chỉ IP có thể bị giả mạo, kẻ tấn công cũng có thể sử dụng những chương trình đặc biệt để xây dựng các gói tin IP có vẻ như xuất phát từ những địa chỉ hợp lệ thuộc mạng nội bộ của một công ty. Sau khi đoạt được quyền truy cập vào mạng bằng IP hợp lệ, kẻ tấn công có thể thực hiện các ý đồ xấu như sửa đổi, định tuyến lại hay xóa dữ liệu hệ thống.

##### 1.1.5. Mô hình tấn công mạng

* Mô hình tấn công truyền thống

Mô hình tấn công truyền thống là mô hình tấn công xuất phát từ một nguồn. từ một đến một hoặc từ một đến nhiều. Có nghĩa là cuộc tấn công xảy ra từ một nguồn gốc.

* Mô hình tấn công phân tán

Mô hình tấn công phân tán sử dụng quan hệ “nhiều đến một” và “nhiều đến nhiều”. Tấn công phân tán dựa trên các cuộc tấn công cổ điển thuộc nhóm từ chối dịch vụ, chính xác hơn là dựa trên các cuộc tấn công như Flood hay Storm (Những thuật ngữ trên có thể hiểu tương tự như “bão”, “Lũ lụt” hay “Thác tràn”)

Diagram

Description automatically generated

# Hình 1.1: Mô hình tấn công phân tán

- Các bước tấn công mạng



Xác định mục tiêu tấn công



Thu thập thông tin, tìm lỗ hổng



Lựa chọn mô hình tấn công

, xây

dựng công cụ



Thực hiện tấn công



Xóa dấu vết (Nếu cần

)



# Hình 1.2: Các bước tấn công mạng

Các kiểu tấn công có nhiều hình thức khác nhau, nhưng thông thường đều thực hiện qua các bước như sau:

+ Xác định mục tiêu tấn công: Xác định rõ mục tiêu tấn công, nơi chuẩn bị tấn công.

+ Thu thập thông tin và tìm lỗ hổng: Khảo sát thu thập thông tin về hệ thống chuẩn bị tấn công bằng nhiều hình thức. Sau khi đã thu thập thông tin, người tấn công sẽ dò tìm những thông tin về lỗ hổng bảo mật của hệ thống dựa trên những thông tin đã thu thập được, phân tích điểm yếu của hệ thống mạng, sử dụng các công cụ hỗ trợ dò quét, tìm lỗi trên hệ thống đó.

+ Lựa chọn mô hình tấn công và công cụ: Khi đã có được những điểm yếu của hệ thống mạng, người tấn công sẽ sử dụng các mô hình phù hợp, lựa chọn một công cụ hoặc tự xây dựng một công cụ để tấn công vào hệ thống.

+ Thực hiện tấn công: Sửa dụng các công cụ hỗ trợ, áp dụng mô hình tấn công đã lựa chọn và các lỗ hổng hệ thống tiến hành tấn công vào hệ thống, Sau khi đã tấn công thành công, khai thác được lỗ hổng của hệ thống. Người tấn công sẽ thực hiện việc duy trì với mục đích khai thác và tấn công trong tương lai gần. Người tấn công có thể sử dụng những thuật như mở cửa sau (backdoor) hoặc cài đặt một trojan để nhằm mục đích duy trì sự xâm nhập của mình. Việc duy trì và làm chủ một hệ thống tạo cho kẻ tấn công có đủ những điều kiện để khai thác, phục vụ những nhu cầu về thông tin. Ngoài ra hệ thống mạng này khi bị chiếm quyền điều khiển cũng sẽ trở thành nạn nhân của một hệ thống botnet được sử dụng trong các cuộc tấn công khác. Ví dụ như tấn công từ chối dịch vụ đến một hệ thống khác.

+ Xóa dấu vết: Khi đã tấn công thành công một hệ thống, người tấn công sẽ cố gắng duy trì sự xâm nhập. Sau đó người tấn công phải làm sao xóa hết dấu vết để không bị phát hiện hoặc không còn chứng cứ pháp lý. Người tấn công có thể xóa các tập tin log, xóa các cảnh báo từ hệ thống phát hiện xâm nhập. Ở các giai đoạn thu thập thông tin và dò tìm lỗ hổng trong bảo mật, người tấn công thường làm lưu lượng trong mạng thay đổi khác với lúc bình thường rất nhiều, đồng thời tài nguyên hệ thống bị ảnh hưởng đáng kể.

Những dấu hiệu này rất có ích cho người quản trị mạng có thể phân tích và đánh giá tình hình hoạt động của hệ thống mạng. Hầu hết các cuộc tấn công đều tiến hành tuần tự như các bước đã nêu trên. Làm sao để biết hệ thống mạng đang bị tấn công, xâm nhập ngay từ hai bước đầu tiên là hết sức quan trọng.  **1.1.6. Một số dấu hiệu phát hiện hệ thống bị tấn công**

* Kiểm tra các dấu hiệu hệ thống bị tấn công: Hệ thống thường bị treo hoặc thường xuyên xuất hiện những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân có phải do phần cứng hay không, nếu không phải rất có thể hệ thống đã bị tấn công [1].
* Kiểm tra tài khoản người dùng mới trên hệ thống: Một số tài khoản lạ, nhất là ID của tài khoản đó bằng 0.
* Kiểm tra sự xuất hiện các tập tin lạ. Thông thường phát hiện sự xuất hiện các tập tin lạ thông qua cách đặt tên các tập tin. Người quản trị hệ thống cần có thói quen đặt tên các tập tin theo quy luật nhất định để dễ đang kiểm soát và phát hiện các tập tin lạ.
* Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình login. - Kiểm tra hiệu năng của hệ thống: Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống.
* Kiểm tra hoạt động của các dịch vụ mà hệ thống cung cấp: Một trong các mục đích tấn công là làm cho tê liệt hệ thống, hình thức tấn công Dos. Sử dụng các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.
* Kiểm tra truy cập hệ thống bằng các tài khoản thông thường, đề phòng trường hợp các tài khoản này bị truy cập trái phép và thay đổi quyền truy cập mà người sử dụng hợp pháp không kiểm soát được.
* Kiểm tra các tệp tin có liên quan đến cấu hình mạng và dịch vụ. Nên loại bỏ các dịch vụ không cần thiết. Nếu không loại bỏ những dịch vụ này nên chạy dưới quyền root, không nên chạy bằng các quyền yếu hơn.

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống.

##### 1.2. Hệ thống phát hiện và ngăn chặn xâm nhập IDS/IPS

###### 1.2.1. Hệ thống phát hiện xâm nhập IDS

Do sự nguy hiển và tổn thất đến từ các cuộc tấn công mạng ngày càng gia tăng nên cần xây dựng một hệ thống phát hiện xâm nhập (IDS) để phát hiện các dấu hiệu bất thường, cảnh báo khi có biểu hiện bất thường và giám sát các hoạt động ra vào hệ thống để phân tích và ngăn chặn kịp thời.

Intrusion Detection Systems (IDS) có thể là một thiết bị phần cứng (các thiết bị phát hiện xâm nhập của Cisco (Cisco IDSM-2 hoặc Cisco IPS 4200 Series Sensors)) hoặc cũng có thể là một ứng dụng phần mềm giúp giám sát máy tính, hệ thống mạng trước các hành động đe dọa đến hệ thống hoặc vi phạm chính sách an ninh và báo cáo lại cho người quản trị hệ thống. Một hệ thống phát hiện xâm nhập cài đặt trên hệ thống mạng giống như một hệ thống cảnh báo chống trộm trong một ngôi nhà.

Một số hệ thống phát hiện xâm nhập còn kiêm luôn cả chức năng ngăn chặn các mối đe dọa đó tuy nhiên điều đó có thể không cần thiết và cũng không phải là chức năng chính của của một hệ thống phát hiện xâm nhập.

Một hệ thống phát hiện xâm nhập cơ bản sẽ “xác định” các mối nguy hại, “ghi” lại thông tin về chúng và sau đó “báo cáo” lại các thông tin đó.

IDS có thể được phân loại theo chức năng thành 2 loại là Network-based IDS và Host-based IDS. Mỗi loại có một cách tiếp cận riêng biệt để theo dõi và bảo vệ dữ liệu và mỗi loại cũng có những ưu nhược điểm riêng.

###### 1.2.2. Network-based IDS

Hệ thống phát hiện xâm nhập dựa trên mạng hoạt động như một thiết bị độc lập trên mạng. Nó thường được đặt ở các segment mạng hoặc các điểm kết nối giữa các vùng mạng khác nhau. Nhờ đó nó có thể giám sát lưu lượng mạng từ nhiều host khác nhau trong vùng mạng đó. NIDS có thể là một thiết bị phần cứng hoặc phần mềm.

Về cấu trúc thì NIDS thường bao gồm một tập hợp các cảm biến (sensors) được đặt ở các điểm khác nhau trong hệ thống mạng. Các cảm biến này sẽ thực hiện giám sát lưu lượng mạng, thực hiện phân tích cục bộ lưu lượng mạng đó và báo cáo về cho trung tâm quản lý (Center Management Console).

# Diagram Description automatically generatedHình 1.3: Mô hình triển khai hệ thống NIDS

Một số NIDS: Snort, Suricata, các NIDS của Cisco, Juniper...

**Ưu điểm của NIDS:**

* Quản lý được cả một network segment (gồm nhiều host). Chi phí thấp vì có thể giám sát cả một hệ thống mạng lớn với chỉ vài thiết bị (mạng được thiết kế tốt). - Phát hiện và đối phó kịp thời: NIDS phát hiện các cuộc tấn công ngay khi xảy ra, vì thế việc cảnh báo và đối phó có thể thực hiện được nhanh hơn. VD: một hacker thực hiện tấn công DoS dựa trên TCP có thể bị NIDS phát hiện và ngăn chặn ngay bằng việc gửi yêu cầu TCP reset nhằm chấm dứt cuộc tấn công trược khi nó xâm nhập và phá vỡ máy bị hại.
* Có tính độc lập với OS (Operating System).
* Phát hiện được các cuộc tấn công mà HIDS bỏ qua: Khác với HIDS, NIDS kiểm tra header của tất cả các gói tin vì thế nó không bỏ sót các dấu hiệu xuất phát từ đây. Ví dụ nhiều cuộc tấn công DoS, TearDrop (phân nhỏ) chỉ được phát hiện khi xem header của các gói tin lưu chuyền trên mạng.

**Nhược điểm của NIDS:**

* NIDS có thể gặp khó khăn trong việc xử lý tất cả các gói tin trên một mạng có kích thước lớn và mật độ lưu thông cao. Điều này dẫn đến NIDS có thể sẽ không thể phát hiện ra một cuộc tấn công khi mạng đang ở trạng thái over-whelming (quá tải). - Bị hạn chế bởi switch. Trên các mạng chuyển mạch hiện đại, các switch được sử dụng nhiều để chia mạng lớn thành các segment nhỏ để dễ quản lý. Vì thế dẫn đến NIDS không thể thu thập được thông tin trong toàn hệ thống mạng. Do chỉ kiểm tra trên segment mà nó kết nối trực tiếp nên nó không thể phát hiện tấn công trên một segment khác. Vấn đề này dẫn đến việc tổ chức phải mua một số lượng lớn cảm biến nếu muốn bao phủ toàn hệ thống mạng của họ, làm tăng chi phí.
* NIDS không thể phân tích được các thông tin đã bị mã hóa (SSL, SSH...). - Một số hệ thống NIDS có thể gặp khó khăn với dạng tấn công phân mảnh gói dự liệu (fragmenting packets).
* NIDS không thể phân biệt được một cuộc tấn công thành công hay thất bại. Nó chỉ có thể phân biệt được có một cuộc tấn công đã được khởi xướng. Điều này nghĩa là để biết được cuộc tấn công đó thành công hay thất bại người quản trị phải điều tra các máy chủ và xác định nó có bị xâm nhập hay không.

###### 1.2.3. Host-based IDS

Hệ thống phát hiện xâm nhập dựa trên máy chủ hoạt động trên một máy trạm đơn. HIDS sẽ sử dụng các tài nguyên của máy chủ đó để theo dõi lưu lượng truy cập và phát hiện các cuộc tấn công nếu có. Bằng cách này HIDS có thể theo dõi được tất cả các hoạt động trên host đó như tập tin log và những lưu lượng mạng ra vào host đó. Ngoài ra nó còn theo dõi hệ điều hành, lịch sử sổ sách, các thông điệp báo lỗi của máy chủ.

Không phải hầu hết các cuộc tấn công đều thông qua hệ thống mạng, nên không phải lúc nào NIDS cũng có thể phát hiện được cuộc tấn công trên một host. Ví dụ, kẻ tấn công có quyền physical access, từ đó có thể xâm nhập vào host đó mà không cần tạo ra bất cứ network traffic nào.

Một ưu điểm của HIDS so với NIDS đó là nó có thể ngăn chặn các cuộc tấn công phân mảnh (Fragmentation Attacks). Bởi vậy nên HIDS thường được cài đặt trên các trên các máy chủ xung yếu của tổ chức, các server trong vùng DMZ (do là mục tiêu tấn công chính).

HIDS cũng thường theo dõi những gì thay đổi trên hệ thống như các thuộc tính của hệ thống tập tin, các thuộc tính (kích thước, vị trí, quyền…) của tập tin, phát hiện tập tin mới được tạo ra hay xóa đi.

Diagram

Description automatically generated

# Hình 1.4: Mô hình hệ thống HIDS

Một số HIDS: Symantec ESM, OSSEC, Tripwire ...

**Ưu điểm của HIDS:**

* Xác định được kết quả của cuộc tấn công: Do HIDS sử dụng dữ liệu log lưu các sự kiện xảy ra, nó có thể biết được cuộc tấn công là thành công hay thất bại với độ chính xác cao hơn NIDS. Vì thế, HIDS có thể bổ sung thông tin tiếp theo khi cuộc tấn công được sớm phát hiện với NIDS.
* Giám sát được các hoạt động cụ thể của hệ thống: HIDS có thể giám sát các hoạt động mà NIDS không thể như: truy nhập file, thay đổi quyền, các hành động thực thi, truy nhập dịch vụ được phân quyền. Đồng thời nó cũng giám sát các hoạt động chỉ được thực hiện bởi người quản trị. Vì thế hệ thống HIDS có thể là một công cụ cực mạnh để phân tích các cuộc tấn công có thể xảy ra do nó thường cung cấp nhiều thông tin chi tiết và chính xác hơn một hệ NIDS.
* Không bị ảnh hưởng bởi các thiết bị chuyển mạch (switch).

**Nhược điểm của HIDS:**

* Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.
* HIDS không thể phát hiện việc quét mạng (network scan bằng nmap) do chỉ giám sát trên host mà nó được cài đặt.
* Có thể bị vô hiệu hóa bởi tấn công từ chối dịch vụ (DoS).
* Chiếm tài nguyên hệ thống: Do cài đặt trên máy cần bảo vệ nên nó sẽ sử dụng tài nguyên của hệ thống như RAM, CPU, Hard Disk dẫn đến có thể làm giảm hiệu suất của việc giám sát.
* HIDS sẽ không hoạt động khi hệ điều hành của host đó lỗi hoặc không hoạt động.

###### 1.2.4. Hệ thống ngăn chặn xâm nhập IPS

Hệ thống ngăn ngừa xâm nhập nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe dọa tấn công bằng việc loại bỏ lưu lượng mạng bất hợp pháp, trong khi vẫn cho phép các hoạt động hợp pháp được tiếp tục.

IPS ngăn chặn các cuộc tấn công dưới những dạng sau:

* Ứng dụng không mong muốn và tấn công kiểu “Trojan horse” nhằm vào mạng và ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và danh sách kiểm soát truy nhập.
* Các tấn công từ chối dịch vụ như “lụt” các gói tin SYN và ICMP bởi việc dùng các thuật toán dựa trên cơ sở “ngưỡng”.
* Sự lạm dụng các ứng dụng và giao thức qua việc sử dụng những qui tắc giao thức ứng dụng và chữ kí.
* Những tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng giới hạn tài nguyên dựa trên cơ sở ngưỡng.

Các sản phẩm IPS không thể nhận biết được trạng thái tầng ứng dụng (chỉ có thể nhận biết được các dòng thông tin trên tầng mạng). Do vậy các cuộc tấn công trên tầng ứng dụng sẽ không bị phát hiện và ngăn chặn.

##### 1.3. Hệ thống giám sát an ninh mạng

###### 1.3.1. Giới thiệu hệ thống giám sát an ninh mạng

Giám sát an ninh mạng là việc thu thập các thông tin trên các thành phần của hệ thống, phân tích các thông tin, dấu hiệu nhằm đánh giá và đưa ra các cảnh báo cho người quản trị hệ thống. Hệ thống giám sát an ninh mạng được triển khai tại các hệ thống mạng có độ nhảy cảm cao hoặc có các thông tin cần bảo mật, hoặc cũng có thể đơn giản chỉ là để theo dõi các diễn biến của mạng [8].

###### 1.3.2. Mô hình giám sát an ninh mạng

Về mô hình giám sát an ninh mạng được triển khai có hai dạng chính: Dạng phân tán và dạng hoạt động độc lập.

- Dạng phân tán: Là mô hình mà trong đó có hệ thống xử lý được đặt ở trung tâm và mọi hoạt động của hệ thống như: Các sự kiện, luồng dữ liệu,… sẽ được xử lý tại trung tâm sau đó được hiển thị lên giao diện Website. Đối với mô hình này thường đòi hỏi một sự đầu tư quy mô cả về thiết bị lẫn con người để vận hành hệ thống này.

Diagram

Description automatically generated

# Hình 1.5: Mô hình giám sát an ninh mạng dạng phân tán

- Dạng hoạt động độc lập: Đây là mô hình mà hệ thống được xây dựng riêng lẻ cho các đơn vị, và không liên quan tới nhau, có nghĩa là hệ thống hoạt động độc lập. Các nhật ký hệ thống và luồng dữ liệu được trực tiếp thu thập tại mạng con, sau đó đẩy về thiết bị giám sát an ninh mạng và tại đây luồng dữ liệu sẽ được xử lý. Tuy nhiên, mô hình này phù hợp cho các ngân hàng và đơn vị nhỏ và yêu cầu về đầu tư và lực lượng con người không cao [8].

Diagram

Description automatically generated

# Hình 1.6: Mô hình giám sát an ninh mạng dạng độc lập

##### 1.3.3. Các công nghệ giám sát an ninh mạng

- Công nghệ NMS (Network Monitoring Solution) là công nghệ tập trung vào các giải pháp quản lý hiệu xuất mạng, giám sát mạng, giám sát tình trạng gói tin, thời gian đáp ứng và số liệu hiệu xuất của các thiết bị như router, switch, các máy chủ... NMS phân tích băng thông tiêu thụ bởi người sử dụng và các ứng dụng thông qua

NetFlow, Sflow, jFlow, FIX ... và đưa ra biểu đồ. Thu thập, phân tích các bản ghi từ tường lửa.

Quản lý các địa chỉ IP sẽ cấp và đã được cấp. Theo dõi các cổng switch và các thiết bị kết nối với nó trong thời gian thực.

Quản trị qua giao diện web và Thiết lập các ngưỡng với nhiều cấp để đưa ra cảnh báo.

Graphical user interface, website

Description automatically generated

# Hình 1.7: Giao diện web của một phần mềm NMS

NMS tối đa hóa độ sẵn sàng cho hệ thống bằng cách giám sát tất cả các thiết bị hoạt động trong hệ thống mạng, bao gồm máy chủ, máy trạm, thiết bị mạng và các ứng dụng. Khi có sự cố, NMS sẽ tự động cảnh báo để nhà quản trị có giải pháp kịp thời. Một số sản phẩm NMS của các nhà cung cấp hàng đầu thế giới còn có khả năng khuyến nghị, hướng dẫn các bước cho nhà quản trị khắc phục sự cố. Giải pháp do hệ thống đưa ra có thể không chính xác 100% vì chỉ là tập hợp kinh nghiệm của các chuyên gia hàng đầu thế giới trong cùng lĩnh vực, nhưng chúng cũng góp phần giảm thiểu thời gian tìm kiếm giải pháp, đặc biệt với các nhà quản trị chưa có nhiều kinh nghiệm. - Công nghệ Siem

Công nghệ quản lý và phân tích sự kiện an toàn thông tin viết tắt là SIEM (Security information and event management – SIEM) là hệ thống được thiết kế nhằm thu thập thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và lưu trữ dữ liệu một cách tập trung. Theo đó, các sản phẩm SIEM cho phép phân tích tập trung và báo cáo về các sự kiện an toàn mạng của tổ chức. Kết quả phân tích này có thể được dùng để phát hiện ra các cuộc tấn công mà không thể phát hiện được theo phương pháp thông thường. Một số sản phẩm SIEM còn có khả năng ngăn chặn các cuộc tấn công mà chúng phát hiện được.

Sản phẩm SIEM đã xuất hiện nhiều năm nay, nhưng tiền thân của sản phẩm này nhắm đến các tổ chức lớn với khả năng và đội ngũ phân tích an ninh chuyên biệt. SIEM đang dần trở nên nổi bật, phù hợp cả với nhu cầu của các tổ chức vừa và nhỏ. Kiến trúc SIEM ngày nay bao gồm phầm mềm SIEM cài đặt trên một máy chủ cục bộ, một phần cứng cục bộ hoặc một thiết bị ảo dành riêng cho SIEM.