LỜI NÓI ĐẦU

Do số lượng xâm phạm ngày càng tăng trên internet và các mạng nội bộ ngày càng xuất hiện nhiều ở khắp mọi nơi, thách thức của vấn đề xâm phạm mạng đã buộc các tổ chức phải bổ sung thêm hệ thống khác để kiểm tra các lỗ hổng về bảo mật. Các hacker và kẻ xâm nhập đã tạo ra rất nhiều cách để có thể thành công trong việc làm sập một mạng hoặc dịch vụ Web của một công ty.

Nhiều phương pháp đã được phát triển để bảo mật hạ tầng mạng và việc truyền thông trên Internet, bao gồm các cách sử dụng tường lửa (Firewall), mã hóa, và mạng riêng ảo (VPN). Hệ thống phát hiện xâm nhập trái phép (IDS-Intruction Detection System) là một phương pháp bảo mật có khả năng chống lại các kiểu tấn công mới, các vụ lạm dụng xuất phát từ trong hệ thống và có thể hoạt động tốt với các phương pháp bảo mật truyền thống.

Với mục tiêu nhằm hạn chế rủi ro có thể xảy ra đối với mạng thông tin của các tổ chức, xây dựng một hệ thống chủ động ngăn ngừa, chống lại những tấn công mạng, nhóm chúng em đã thực hiện đề tài nghiên cứu và xây dựng hệ thống mạng Lan bảo mật nhằm trang bị cho mạng thông tin của một tổ chức, công ty hoặc nhà cung cấp dịch vụ Internet.

LỜI CẢM ƠN

Chúng em xin chân thành cám ơn TS. Hồ Khánh Lâm đã giúp đỡ chỉ bảo tận tình trong quá trình hoàn thành đồ án này. Chúng em cũng xin cám ơn các bạn học, thầy cô trong khoa Công Nghệ Thông Tin đã giúp đỡ trao đổi góp ý trong thời gian chúng em làm đồ án.

Chung em xin gửi lời cam ơn tới gia đinh, bạn bè đã động viên, cung cấp tài liệu và đóng góp ý kiến cho chúng em trong suốt thời gian thực hiện đề tài

Cuối cùng xin cám ơn khoa Công Nghệ Thông Tin trường Đại Học Sư Phạm Kỹ Thuật Hưng Yên đã giúp đỡ ủng hộ nhóm em hoàn thành tốt đồ án tốt nghiệp .

Do kinh nghiệm chưa nhiều, đây lại là một đề tài mới nên nhóm chúng em trong quá trình làm, và hoàn thành đồ án không tránh khỏi những sai lầm, thiếu sót. Vậy nên, rất mong có được sự đóng góp ý kiến của bạn đọc, thầy cô và bạn bè.

Chúng em xin chân thành cảm ơn !

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, VIẾT TẮT

Từ viết tắt	Từ viết đầy đủ
ACID	Analysis Console for Intrusion Databases
ACL	Access Control List
AH	Authentication Header
DdoS	Distributed Deny of Service
DNS	Domain Name Service
DoS	Deny of Service
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection System
HTML	Hyper Text Mark Language
ICMP	Internet Control Message Protocol
IDES	Intrusion Detection Expert System
IDS	Intrusion Detection System
IP	Internet Protocol
ISO	International Stadard Organization
LDAP	Lightweight Directory Access Protocol
NFS	Network File Sharing
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NOS	Network Operation System
OS	Operation System
OSI	Open Systems Interconnection
PGP	Pretty Good Privacy
SMTP	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SQL	Sequence Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

PHẦN I: MỞ ĐẦU

I. Lý do chọn đề tài

Chúng em thực hiện đồ án này với mong muống không chỉ nghiên cứu những đặc trưng cơ bản của hệ thống phát hiện xâm nhập trái phép với vai trò là một phương pháp bảo mật mới bổ sung cho những phương pháp bảo mật hiện tại, mà còn có thể xây dựng được một phần mềm IDS phù hợp với điều kiện của Việt Nam và có thể ứng dụng vào thực tế nhằm đảm bảo an toàn cho các hệ thống và chất lượng dịch vụ cho người dùng.

IDS không chỉ là công cụ phân tích các gói tin trên mạng, từ đó đưa ra các cảnh báo đến nhà quản trị mà nó còn cung cấp những thông tin sau:

- Các sự kiện tấn công.
- Phương pháp tấn công
- Nguồn gốc tấn công.
- Dấu hiệu tấn công

Loại thông tin này ngày càng trở nên quan trọng khi các nhà quản trị mạng muốn thiết kế và thực hiện chương trình bảo mật thích hợp cho một tổ chức riêng biệt

Một số lý do để thêm IDS cho hệ thống tường lửa là:

- Kiểm tra hai lần nếu hệ thống tường lửa sai
- Ngăn chặn các cuộc tấn công được cho phép thông qua tường lửa
- Làm cho nỗ lực tấn công bị thất bại.
- Nhận biết các cuộc tấn công từ bên trong.

II. Phân tích hiện trạng

- 04/7/2002, Viện An ninh máy tính đã báo cáo có đến 80% thiệt hại tài chính vượt qua 455 triệu đôla bị gây ra bởi sự xâm nhập và mã nguy hiểm

- Hàng triệu công việc bị ảnh hưởng do sự xâm nhập.

- Nếu sử dụng một phần mềm chống virut thì bạn phải xem xét đến việc bổ sung thêm một IDS cho chiến lược bảo mật của mình. Hầu hết các tổ chức sử dụng phần mềm chống virut không sử dụng IDS.

- Ngày nay do công nghệ ngày càng phát triển nên không có một giải pháp bảo mật nảo có thể tồn tại lâu dài. Theo đánh giá của các tổ chức hàng đầu về công nghệ thông tin trên thế giới, tình hình an ninh mạng vẫn trên đà bất ổn và tiếp tục được coi là năm " bất động đỏ" của an ninh mạng toàn cầu kho có nhiều lỗ hổng an ninh nghiêm trọng được phát hiện, hình thức tấn công thay đổi và có nhiều cuộc tấn công của giới tội phạm công nghệ cao vào các hệ thống công nghệ thông tin của các doanh nghiệp.

- Lấy ví dụ với hệ điều hành vista có thể bị tấn công bởi một lỗ hổng " blue screen of death" hay vẫn thường được gọi là manh hình xanh chết chóc. Hacker có thể gửi tới hệ thống một yêu cầu chứa các mã lệnh tấn công trực tiếp vào hệ thống của Vista và làm ngưng hoạt mọi động

- Hệ thống phát hiện xâm nhập trái phép IDS là một phương pháp bảo mật có khả năng chống lại các kiểu tấn công mới, các vụ lạm dụng, dùng sai suất từ trong hệ thống và có thể hoạt động tốt với các phương pháp bảo mật truyền thống. Nó đã được nghiên cứu, phát triển, và ứng dụng từ lâu trên thế giới và đã thể hiện vai trò quan trọng trong các chính sách bảo mật.

a. Xác định nhiệm vụ bắt buộc

- Yêu cầu bắt buộc:

1. IDS là gì?

2. Các thành phần của IDS.

3. Các mô hình IDS

4. Các ứng dụng IDS phổ biến hiện nay.

5. Triển khai mô hình IDS demo trong mạng LAN

- yêu cầu mở rộng:

Xây dựng ứng dụng demo thành phần cảm biến và cảnh báo của một IDS

b. Giới hạn và phạm vi nghiên cứu

- Tìm hiểu hệ thống mạng máy tính cục bộ của các tổ chức, doanh nghiệp và có tham gia kết nối internet.

- Tìm hiểu các nguy cơ xâm nhập trái phép đối với hệ thống mạng.

- Tình hiểu các kỹ thuật của việc phát hiện và ngăn chặn xâm nhập

- Tìm hiểu Cisco-IDS Sofware.

c. Phương pháp nghiên cứu

- Nghiên cứu lý luận

Dựa vào kiến thức bảo mật và an ninh đã được tịch lũy trong quá trình học tập, cộng với sự tham khảo tài liệu của bạn bè, hệ thống internet và đặc biệt là của các thầy cô trong bộ môn. Nhóm đã tìm hiểu và đi sâu được vào nội dung của đề tài này.

- Nghiên cứu thực tiễn

Trên thị trường hiện nay đã có nhiều sản phẩm Cisco IDS được hoàn thành và chứng nhận như: Intrust, ELM, GFI LANGUARD S.E.L.M, Snort, Dragon. Dựa trên việc tìm hiểu và nghiên cứu các sảm phẩm tương tự đã có trên để đưa ra phân tích, đánh giá và nghiên cứu hệ thống riêng của nhóm

d. Ý nghĩa thực tiễn của đề tài

- Nghiên cứu các vấn đề kỹ thuật của hệ thống phát hiện và ngăn chặn xâm nhập.

- Phân tích, đánh giá được các nguy cơ xâm nhập trái phép đối với hệ thống mạng.

- Đưa ra một số giải pháp an ninh hữu hiệu cho hệ thống mạng tổ chức, doanh nghiệp.

Trong đồ án này, chúng em phân tích đánh giá những rủi ro an ninh của mạng, cách thức tấn công và bảo vệ mạng, hiệu quả của các phương pháp tự động dò tìm tấn công sử dụng cho hệ thống dò tìm xâm nhập IDS. Từ đó xây dựng mô hình hệ thống IDS cho một mạng LAN đơn giản nhằm phòng chống và ngăn ngừa các tấn công mạng dưới một số hình thức phổ biến. Đồ án được chia làm 4 chương cụ thể như sau:

Chương I: Tổng quan về an ninh mạng. Trình bày tổng quan về an ninh mạng, mục tiêu của chính sách an ninh mạng và cách thức xây dựng chính sách an ninh. Chương này chủ yếu tập trung vào phân tích rủi ro, lỗ hổng của mạng; cách thức tấn công, nhược điểm của giao thức TCP/IP và phương pháp bảo vệ mạng khỏi tấn công.

Chương II: Nêu ra hàng loạt các phương thức tấn công phổ biến ngày nay bao gồm: Khái niệm, nguyên lý tấn công và cách ngăn ngừa, phòng chống chúng.

Chương III: Hệ thống IDS. Trình bày kiến thức về hệ thống dò tìm xâm nhập (IDS), cấu trúc hệ thống, phương pháp phân loại, cách thức dò tìm xâm nhập và phương pháp xử lý dữ liệu.

Chương IV: Xây dựng mô hình mạng LAN cơ bản có IDS bảo vệ được kết nối internet . Chương này tập trung chủ yếu demo các nguyên lý tấn công mạng, cách tấn công và phương pháp phòng chống. Trình bày mô hình, cấu trúc, và một số kết quả thu được hệ thống IDS thử nghiệm cho một mạng LAN.

PHẦN II: NỘI DUNG

CHƯƠNG I: TỔNG QUAN VỀ AN NINH MẠNG

1.1. Giới thiệu về an ninh mạng, sự cần thiết của an ninh mạng

1.1.1. Sự cần thiết của an ninh mạng

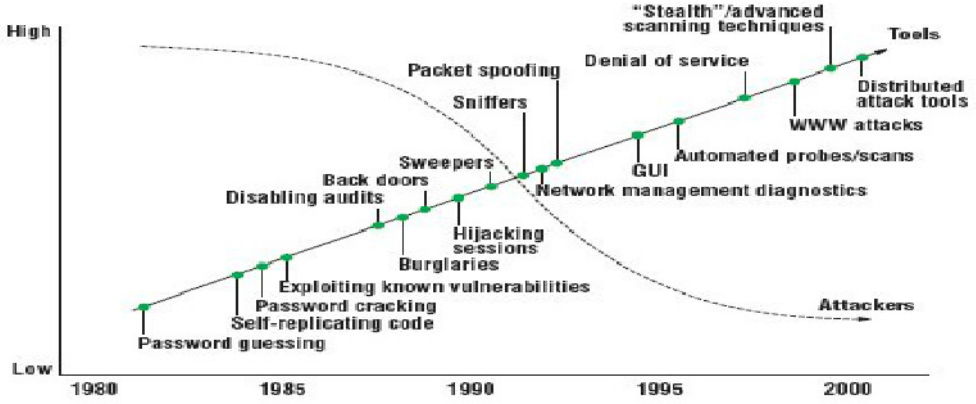
Trong vài năm gần đây, vấn đề an ninh mạng được nhiều tổ chức quan tâm. Ban đầu, các nhà quản trị mạng đều cho rằng sẽ không xảy ra rủi ro nào đối với mạng của mình, tuy nhiên dần dần người ta thấy rằng điều đó có thể xảy ra với bất kỳ hệ thống mạng nào. Các dữ liệu ngày càng lớn và trở nên quan trọng, do đó sẽ trở thành mục tiêu tấn công của những phần tử xấu.

Theo báo cáo thông kê của các tổ chức an ninh mạng tại Mỹ, năm 2003 có tới 90% các báo cáo của các tổ chức, các viện, các trường đại học là họ có tìm thấy lỗi an ninh trong mạng của họ, có tới 70% báo cáo cho rằng các lỗi đó gây nguy hiểm hơn cả virus máy tính và có tới 42% báo cáo cho rằng do lỗi an ninh mạng mà gây tổn thất về tài chính cho tổ chức của họ.

Rất nhiều công ty, tổ chức đang tăng trưởng các ứng dụng thương mại điện tử trên mạng. Việc thiết lập các ứng dụng này cho phép đưa thông tin và các công việc của họ lên mạng internet. Công việc của con người cũng thay đổi theo, ngày nay các nhân viên có thể làm việc ngoài giờ, kéo dài thời gian làm việc hơn hoặc có thể làm việc từ xa, những công việc đó đòi hỏi phải truy nhập mạng để lấy thông tin từ ngoài tổ chức. Ngày nay công việc của nhiều tổ chức, công ty phụ thuộc khá lớn vào hệ thống thông tin. Trong môi trường làm việc như vậy, việc tăng cường kết nối giữa các hệ thống mạng càng trở nên cần thiết. Thông tin được bảo vệ cẩn trọng hơn, và luôn phải đảm bảo tính sẵn sàng trên hệ thống. Những công nghệ mới của thông tin, viễn thông cho phép tăng cường trao đổi thông tin giữa các mạng, đạt được hiệu quả cao hơn trong công việc mà giảm được chi phí. Tuy nhiên đổi lại độ rủi ro về thông tin và rủi ro công việc cũng cao hơn.

Các kỹ thuật tấn công mạng liên tục biến đổi không ngừng, Trong vòng

khoảng hai mươi năm qua, các công cụ tấn công ngày càng trở nên mạnh hơn và dễ sử dụng hơn. Do các công cụ trở nên dễ sử dụng mà những kẻ tấn công nhiều khi không cần tìm hiểu quá sâu về hệ thống cũng có thể thực hiện hành động tấn công mạng. Nhiều chương trình được lập trình sẵn cho phép người tấn công mạng mà không cần hiểu kỹ thuật bên trong như thế nào.



Hình 1.1 – Sự phát triển các kỹ thuật tấn công mạng

Các lỗi an ninh trên mạng cũng được phổ biến rộng rãi trên internet và trong các tạp chí về an ninh mạng. Đây là điều thuận lợi cho những người quản lý mạng thông tin. Để đạt được một mạng thông tin hoạt động có hiệu quả và an toàn, người quản trị có thể thực hiện theo các bước được định sẵn đồng thời đưa ra các chính sách an ninh để cung cấp cho các chương trình xây dựng và duy trì hoạt động cho toàn mạng. Tuy nhiên việc phổ biến kiến thức rộng rãi cũng có hai mặt: Một mặt giúp những nhà quản trị mạng nắm được kiến thức an ninh mạng để có thể xây dựng được một mạng có tính bảo mật cao. Mặt khác những kiến thức này cũng giúp những kẻ tấn công hiểu được hoạt động của hệ thống an ninh và từ đó có thể thực hiện những hành động tấn công dễ dàng.

Một chương trình an ninh mạng cần phải có các yếu tố như: kiến thức an ninh mạng; dò tìm tấn công; bảo mật thông tin; đo lường kiểm tra; quản trị và phản ứng để giảm thiểu tối đa các rủi ro đã xảy ra hoặc có thể xảy ra. Không có một hệ thống an ninh nào là hoàn hảo, một kẻ tấn công có thể vượt qua được hầu hết các hệ thống an ninh. Hệ thống an ninh mạng chỉ có ý nghĩa làm giảm rủi ro và quản lý

được rủi ro.

- Kiến thức về an ninh mạng: là một yêu cầu đối với các nhân viên.

Mọi nhân viên phải hiểu được tại sao họ cần quan tâm đến vấn đề an ninh thông tin. Ví dụ những người dùng đầu cuối thường có xu hướng chọn mật khẩu sao cho dễ nhớ và đơn giản, nhưng họ không biết được rằng đó là một nguy cơ dẫn đến mất an toàn thông tin. Vì thế những người quản lý cần tạo ra những tài liệu, những đợt huấn luyện để cung cấp cho mọi nhân viên kiến thức cơ bản về an ninh mạng, an ninh thông tin.

- Bảo vệ thông tin: phải được làm một cách có hiệu quả. Đầu tiên, chúng ta phải xác định được những thông tin cần bảo vệ và giá trị của những thông tin đó. Xác định nguy cơ có thể xảy ra và những rủi ro chắc chắn sẽ xảy ra đối với lượng thông tin đó. Để xác định cách thức bảo vệ thông tin, chúng ta cần quan tâm tới giá trị của phương thức bảo vệ với giá trị của thông tin cần bảo vệ. Ví dụ chúng ta không cần giành nhiều thời gian và tiền bạc hơn để bảo vệ lượng thông tin quảng cáo so với thông tin khách hàng.
- Dò tìm tấn công: để tìm những hành động tấn công mạng. Nếu chúng ta không thường xuyên theo dõi hệ thống thì không thể tìm ra được những hành động tấn công. Rất nhiều hệ thống có thể cung cấp được các thông tin chi tiết về trạng thái của hệ thống trong nhật ký hệ thống (log file). Chúng ta cần đảm bảo ghi đầy đủ thông tin về hệ thống để truy tìm và nhận dạng được các hành động tấn công. Ngoài ra có thể sử dụng hệ thống dò tìm tấn công tự động (IDS).
- Khôi phục hệ thống: là hành động rất quan trọng để bảo vệ mạng, phản ứng lại các cuộc tấn công mạng. Khi có một kế hoạch đầy đủ, chúng ta có thể xác định được những hành động cần thiết khi có xảy ra những rủi ro trên mạng. Một kế hoạch rõ ràng, chi tiết sẽ giúp chúng ta tiết kiệm được chi phí, tiết kiệm thời gian, giảm thiểu rủi ro.
- Quản trị an ninh mạng: một yêu cầu cần thiết và bắt buộc đối với những mạng có quy mô lớn và phức tạp. An ninh mạng chỉ tốt khi chúng ta có đầy đủ các công cụ quản trị để tạo, cung cấp, kiểm tra việc cấu hình và thực hiện các chính sách an ninh thông tin cho mạng.

Khái niệm về an ninh mạng rất rộng, nó có thể khác nhau đối với nhiều tổ chức, phụ thuộc vào chức năng, mục tiêu và quy mô của các tổ chức. An ninh mạng được thực hiện bởi những thiết bị bảo vệ mạng, những chính sách bảo vệ tài nguyên mạng khỏi những xâm nhập trái phép hoặc làm thay đổi dữ liệu.

Một điều dễ nhận ra là có mối liên hệ mật thiết giữa nhu cầu công việc và bảo mật mạng. Chỉ có một cách duy nhất để máy tính an toàn tuyệt đối là ngắt nó ra khỏi mạng và đặt vào một môi trường hoàn toàn có độ bảo mật cao. Tất nhiên với cách thức như vậy sẽ làm giảm khả năng chia sẻ tài nguyên trên hệ thống và giảm tính hiệu quả, năng suất của công việc. Mục đích của anh ninh mạng là làm thế nào để xác định được rủi ro và đưa ra giải pháp giảm tối đa rủi ro đó. Một trong những cách đó là tạo lập được một chính sách an ninh tốt cho toàn bộ mạng.

1.1.2. Các chính sách an ninh chung

Chính sách an ninh mạng được tạo ra dựa trên mục đích bảo vệ thông tin của từng tổ chức. Những nhân viên kỹ thuật sẽ sử dụng chính sách này để thiết kế và thực hiện vấn đề an ninh cho mạng lưới. Chính sách an ninh của một tổ chức thông thường là những quy định, những điều cấm khi truy nhập vào mạng lưới của tổ chức đó.

Chính sách an ninh không phải là những văn bản mang tính kỹ thuật, mà thông thường là những văn bản mang tính nghiệp vụ dựa vào những quy định đối với những hành động được phép hay không được phép để đảm bảo an ninh cho mạng. Chính sách an ninh không quy định cụ thể những công việc phải thực hiện mà nó chỉ xác định phạm vi ảnh hưởng của chính sách. Thông thường, các chính sách an ninh được chia thành những chủ đề phạm vi nhỏ hơn, ví dụ: “chính sách chấp nhận sử dụng” quy định những quyền và trách nhiệm của người sử dụng khi truy nhập, sử dụng những tài nguyên thông tin của tổ chức. Việc phân chia phạm vi phụ thuộc vào độ lớn của từng tổ chức, tuy nhiên có một số chính sách sau đây được sử dụng rộng rãi trong hầu hết các tổ chức:

- Chính sách chấp nhận sử dụng: Quy định những hành động được phép và không được phép khi một người sử dụng muốn truy nhập vào mạng hoặc sử dụng dịch vụ

của một tổ chức. Những hành động này người sử dụng phải đồng ý (chấp nhận) khi tham gia vào mạng của tổ chức đó.

- Chính sách thiết lập cấu hình cho thiết bị: Quy định cấu hình tối thiểu bắt buộc đối với các máy chủ, máy trạm, thiết bị mạng khi hoạt động trên mạng để đảm bảo an toàn và bảo mật thông tin của tổ chức.
- Chính sách quản lý phần mềm: Chính sách này xác định quyền sử dụng các phần mềm, vấn đề bản quyền đối với các sản phẩm ….
- Chính sách hạ tầng mạng lưới: Chính sách này đưa ra những quy định về quản lý cơ sở hạ tầng mạng lưới, quy định ai là người có trách nhiệm.
- Chính sách quản lý tài khoản: Quy định quyền của từng tài khoản, giới hạn sử dụng của quyền đó. Ngoài ra chính sách này còn xác định cả môi trường làm việc của từng loại tài khoản…

Các bước thiết lập chính sách an ninh

Có nhiều cách để thiết lập chính sách an ninh cho mạng, tùy theo mục đích, quy mô của từng tổ chức. Tuy nhiên có thể thực hiện theo ba bước cơ bản sau để thiết lập chính sách an ninh.

- Chuẩn bị: Khi thiết lập một chính sách an ninh, đầu tiên chúng ta nên thực hiện liệt kê những chính sách đó ra văn bản. Tiếp theo thực hiện phân tích những rủi ro và đánh giá mức độ của rủi ro. Và sau đó là thiết lập các đội kỹ thuật và quy định trách nhiệm cho họ.
- Phòng chống: Bước này xác định xem làm thế nào để chúng ta có thể thực hiện được chính sách an ninh đã đề ra. Ngoài ra chúng ta cũng cần quản lý, theo dõi công việc thực hiện đó, ví dụ như việc ghi nhật ký hệ thống, phân tích dữ liệu…
- Đáp ứng: Bước này quy định những hành động cần làm khi xảy ra sự cố đối với mạng, quy định cả trách nhiệm và quyền hạn của từng thành viên để đưa ra được những quyết định nhanh nhất nhằm tránh, hạn chế đến mức nhỏ nhất rủi ro cho mạng.

Việc thiết lập chính sách an ninh là công việc phức tạp, đòi hỏi phải có sự

tham gia của những thành viên trong đội ngũ quản lý. Không thể có được một chính sách an ninh tốt nếu không có sự hỗ trợ đầy đủ từ phía quản lý.

Mục tiêu của chính sách an ninh

- Chính sách an ninh là văn bản hướng dẫn cho người kỹ thuật lựa chọn thiết bị sao cho phù hợp, và không chỉ định thiết bị, vì chính sách an ninh không phải là những tài liệu kỹ thuật.
- Mục đích thứ hai của chính sách an ninh là văn bản hướng dẫn việc thiết lập cấu hình để đảm bảo an ninh cho toàn bộ mạng.
- Mục đích thứ ba là xác định trách nhiệm và quyền của người dùng cũng như người quản lý khi tham gia vào mạng.

Nhìn chung mục đích của chính sách an ninh là nguyên tắc, hướng dẫn được sử dụng bởi người quản lý trong việc định ra kế hoạch an ninh mạng sao cho có hiệu quả. Trách nhiệm của người dùng và người quản trị được xác định đầy đủ và rõ ràng.

1.2. Những rủi ro, lỗ hổng của mạng

Hệ máy tính đã trở thành một bộ phận của hầu hết các công ty, tổ chức. Nhiều tập đoàn lớn và các tổ chức chính phủ đã dành một khoản đầu tư lớn để duy trì hoạt động mạng và thậm chí những tổ chức nhỏ nhất cũng sử dụng máy tính để lưu giữ báo cáo về tài chính. Những hệ thống này có thể hoạt động nhanh và chính xác và nó cũng làm cho việc liên lạc giữa các tổ chức trở nên dễ dàng hơn, vì thế hệ thống máy tính ngày càng phát triển và được mở rộng hơn. Bất kỳ tổ chức nào muốn cung cấp thông tin rộng rãi đều có kết nối tới mạng Internet. Truy nhập này mặc dù rất có ích cho công việc nhưng cũng hàm chứa những rủi ro.

Tất cả các mạng máy tính đều chứa cả dữ liệu riêng và dữ liệu có thể công khai. Một kế hoạch an ninh tốt phải bảo vệ được dữ liệu trên mạng bao gồm cả việc cho phép truy nhập đến dữ liệu công khai dưới quyền không có khả năng thay đổi (read only), ví dụ như trang website của một tập đoàn. Một loại dữ liệu khác như tiền lương không cần công khai nhưng phải được hạn chế cho một số người đặc biệt có thể truy nhập được. Một kế hoạch an ninh hoàn hảo cần đảm bảo dữ

liệu của tổ chức, hạn chế tối đa những truy nhập không hợp pháp, đảm bảo hệ thống được sử dụng như mục đích dự kiến. Ngoài ra còn phải đảm bảo mạng này không trở thành nơi cho những kẻ tấn công dùng để tấn công mạng khác.

Những rủi ro, lỗ hổng của mạng thường được tạo ra chủ yếu do các lý do sau:

- Chính sách an ninh kém hiệu quả.
- Lỗi trong quản trị, cấu hình mạng.
- Lỗi trong thiết bị mạng, hệ thống.
- Lỗi do công nghệ, lỗi phần mềm.

1.2.1. Chính sách an ninh chưa tốt

Chính sách an ninh mạng ảnh hưởng trực tiếp tới quá trình thiết kế, triển khai và hoạt động của mạng, đây là điều cơ bản ảnh hưởng tới an ninh mạng. Chính sách an ninh kém hiệu quả có rất nhiều lý do, bao gồm những lý do sau:

- Tính chính trị: Tính chính trị trong một tổ chức có thể tạo ra tính kém hiệu quả trong sự kiên định của một chính sách an ninh, hoặc rất tệ là sự không đồng nhất khi áp dụng chính sách. Rất nhiều chính sách tạo ra một ngoại lệ cho những người quản lý và công việc của họ, những chính sách an ninh như vậy đều không có ý nghĩa khi áp dụng.
- Chính sách thiếu: Một chính sách an ninh viết thiếu không khác gì là không có. Việc xuất bản và phổ biến rộng rãi chính sách an ninh này sẽ làm hỗn loạn trong hoạt động của mạng trong tổ chức.
- Thiếu tính liên tục: Chính sách nhân sự trong tổ chức có thể liên tục thay đổi, vì vậy cần có sự theo dõi để đảm bảo chính sách an ninh luôn được thực hiện trong tổ chức. Khi một người quản lý rời khỏi vị trí của mình cần bàn giao lại toàn bộ quyền và mật khẩu, đồng thời những mật khẩu đó cũng phải được đổi bởi người quản lý mới.
- Thiếu kế hoạch khôi phục hệ thống: Một kế hoạch khôi phục hệ thống tốt phải bao hàm cả những thảm họa bất ngờ sẽ tránh được những điều rắc rối sau thảm họa với khách hàng hay tòa án...
- Thiếu quản lý những bản vá lỗi chương trình trong chính sách an ninh: Một

chính sách an ninh tốt cần có kế hoạch thường xuyên cung cấp những bản sửa lỗi và nâng cấp cho phần cứng và phần mềm. Một thủ tục chi tiết phải được tiến hành với thiết bị mới khi đưa vào hoạt động để đảm bảo tính an ninh cho thiết bị và sản phẩm đó.

- Thiếu theo dõi: Thiếu sự theo dõi thường xuyên tới hoạt động của hệ thống sẽ dẫn đến những cuộc tấn công mạng mà không có phản ứng từ quản trị mạng.
- Thiếu điều khiển truy nhập hợp lý: Một truy nhập bất hợp pháp có thể xảy ra đối với những mạng không có giải pháp hạn chế truy nhập hợp lý. Ví dụ như mật khẩu quá ngắn, không đổi mật khẩu thường xuyên, mật khẩu được dùng chung cho nhiều người…

1.2.2. Thực hiện quản trị, cấu hình mạng chưa tốt

Khi các thiết bị, phần mềm ngày càng trở nên phức tạp, lượng kiến thức đòi hỏi đối với người quản trị cũng tăng theo. Điều này trở thành vấn đề khá nan giải đối với những tổ chức nhỏ nơi mà người quản trị mạng có trách nhiệm đối với nhiều hệ thống khác nhau:

- Không thực hiện cấu hình thiết bị: Một lỗi cấu hình đơn giản có thể gây ra lỗi an ninh mạng nghiêm trọng. Dù lỗi là do thiếu kiến thức hay do lỗi gõ nhầm… thì hậu quả cũng là tạo nên một mạng không an toàn. Một số cấu hình thường gây lỗi là cấu hình điều khiển truy nhập (access list), cấu hình SNMP...
- Mật khẩu yếu hoặc dễ dàng đoán được: Mật khẩu quá ngắn, dễ đoán hoặc chỉ chứa những cụm từ thông dụng thường dễ bị những kẻ tấn công lợi dụng để truy nhập vào mạng, hệ thống. Một mật khẩu được thiết lập phải tuân theo chính sách về đặt mật khẩu để đảm bảo an ninh cho mạng.
- Thiết lập cấu hình dịch vụ thiếu: Các dịch vụ mạng như ứng dụng java, web, ftp thường được thiết lập cấu hình mà không quan tâm đến tính an toàn. Một yêu cầu đối với người quản trị mạng là phải biết rõ những yêu cầu của dịch vụ, những dịch vụ đang chạy trên hệ thống để không tạo ra lỗ hổng an ninh.
- Sử dụng cấu hình mặc định: Cấu hình mặc định thường được thiết lập với mọi thiết bị mới và được ghi lại trong tài liệu. Việc thiết lập cấu hình mặc định cho thiết

bị sẽ gây ra rủi ro cho mạng.

- Rò rỉ thông tin: Những thông tin về cấu hình mạng, cấu trúc hệ thống có thể trở thành thông tin mật và có thể bị đem bán hoặc vô tình để lộ. Những kẻ tấn công có thể lợi dụng những thông tin này tiến hành các cuộc tấn công một cách hoàn hảo không để lại dấu vết. Việc lưu giữ những thông tin này cần được kiểm soát bằng những chính sách an ninh một cách chặt chẽ.

Khi thực hiện cấu hình, người quản trị cần phải lưu ý:

- Có kế hoạch cẩn thận trước khi thiết lập cấu hình.
- Có đấy đủ kiến thức về cấu hình thiết bị đó.
- Dành thời gian để thiết lập cấu hình thiết bị một cách tốt nhất.

1.2.3. Thiết bị mạng có tính an ninh chưa tốt

Có thể miêu tả những thiết bị này là dễ dàng xâm nhập, dễ bị tấn công, không sử dụng những giải pháp điều khiển truy nhập, lọc gói...

- Giao tiếp mạng (Network Interface Card): Thông thường một giao tiếp mạng chỉ nhận những gói tin gửi tới đích có địa chỉ vật lý xác định, những gói tin khác đều bị loại bỏ. Tuy nhiên giao tiếp mạng có khả năng hỗ trợ hoạt động ở trạng thái nghe, cho phép nhận toàn bộ gói tin đến và đi qua giao tiếp mạng đó. Hầu hết các hệ điều hành đều cho phép các chương trình ứng dụng thiết lập chế độ này cho các giao tiếp mạng. Từ đó người sử dụng có thể dễ dàng xem, đọc toàn bộ thông tin đi qua giao tiếp mạng đó.
- Topology của mạng: Mạng chia sẻ rất dễ gây rủi ro, vì toàn bộ lưu lượng mạng nhìn thấy được bởi các thiết bị trên mạng. Những thông tin có tính nhạy cảm như mật khẩu, email, mã thẻ có thể bị lấy trộm một cách dễ dàng. Để khắc phục nhược điểm này, các thiết bị switch đều có tính năng mạng LAN ảo, SPAN để hạn chế khả năng thu nhận toàn bộ gói tin trên mạng chia sẻ. Ngày nay hầu hết các tổ chức đều đang chuyển dần từ các thiết bị chia sẻ tài nguyên sang switch.
- Modem: Việc thiết lập sẵn một modem tạo điều kiện thuận lợi cho việc truy nhập mạng. Tuy nhiên nếu không thực hiện được kiểm soát, modem sẽ trở thành một mục tiêu tấn công, vì rất nhiều thiết bị modem có khả năng thiết lập chế độ

trả lời tự động, đây là lỗ hổng của thiết bị để những kẻ xâm nhập có thể lợi dụng để xâm nhập vào hệ thống.

- Router: Bộ định tuyến hoạt động ở lớp mạng có nhiệm vụ định tuyến và lọc các gói tin. Thông thường router có chức năng kết nối giữa các mạng LAN nên thường xuyên phải chịu tấn công truy nhập mạng và đặc biệt là tấn công DoS.
- Firewall và Proxy: Có chức năng hoạt động như một hệ thống gateway để bảo vệ tài nguyên trong mạng, có nhiệm vụ ngăn cản các tấn công từ mạng ngoài vào mạng trong, Firewall thường sử dụng các cơ chế lọc gói để hoạt động, vì thế các lỗi phổ biến xảy ra là lỗi tràn bộ đệm. Ngoài ra firewall thường bỏ qua các cuộc tấn công từ mạng trong (mạng tin cậy), điều này là rất nguy hiểm với những tấn công vào thẳng hệ thống firewall trong nội bộ mạng. Để đảm bảo hoạt động tin cậy, hệ thống firewal cần thường xuyên được cập nhật những bản sửa lỗi, các luật hoạt động và được theo dõi thường xuyên từ người quản trị.

1.2.4. Các lỗi do công nghệ, phần mềm gây ra

Mỗi một công nghệ đều có những điểm yếu, những điểm yếu này có thể tồn tại trong hệ điều hành, giao thức hay thiết bị mạng.

Khiếm khuyết của thiết bị mạng

Bất kỳ nhà sản xuất nào cung hứa cung cấp những thiết bị tốt nhất, tuy nhiên mọi sản phẩm đều tồn tại sự phức tạp và lỗ hổng trong khi thiết kế. Ngoài ra bất kỳ thiết bị nào cũng có những điểm mạnh và điểm yếu. Một thiết bị có thể hoạt động tốt và an toàn trong môi trường mạng này, nhưng lại không hỗ trợ hay hoạt động kém hiệu quả trong môi trường mạng khác. Vì thế điều quan trọng là phải xác định được loại thiết bị nào hoạt động tốt nhất trong môi trường mạng của mình.

Lỗi hệ điều hành, lỗi phần mềm ứng dụng

Ở đây, phần mềm là khái niệm bao gồm cả hệ điều hành và các gói phần mềm ứng dụng chạy trên hệ điều hành đó. Hầu hết các phần mềm đều có lỗi do nhiều nguyên nhân chủ quan và khách quan.

• Quét lỗi mạng: Các chương trình phần mềm quét mạng thường sử dụng các nguyên lý sau để thực hiện quét:

- Packet In groper (ping): để lấy địa chỉ IP của thiết bị mạng.
- SNMP: Một thiết bị mạng có cấu hình snmp chưa được bảo vệ sẽ trở nên rất nguy hiểm, vì những kẻ xâm nhập có thể sửa đổi được cả cấu hình mạng thông qua thiết bị đó.
- TCP/UDP port: Chương trình quét toàn bộ những cổng dịch vụ và xác định dịch vụ nào đang hoạt động trên mạng, thậm chí chi tiết về từng sản phẩm và lỗi của sản phẩm đó.
- Solarwind: là một chương trình có thể quét toàn bộ mạng, đưa ra những thông báo chi tiết về cả sản phẩm, tài khoản, và có thể phá được cả mật khẩu.
- Nmap: Là một công cụ sử dụng cho các máy tính có dùng hệ điều hành UNIX để quét những mạng lớn. Công cụ này còn có khả năng cho phép vượt qua cả tường lửa, sử dụng cả TCP SYN, ICMP và xác định chi tiết hệ điều hành đang hoạt động trên máy đích.

• Tràn bộ đệm: Các lỗi phần mềm phổ biến hiện nay là lỗi tràn bộ đệm. Việc nhập vào một giá trị không mong muốn có thể gây ra lỗi chương trình, giúp cho những kẻ tấn công có thể xâm nhập vào hệ thống.

- Bộ đệm là một vùng nhớ có giới hạn về kích thước sử dụng cho phần mềm. Nếu bộ đệm đạt tới giới hạn tổng, một lỗi tràn bộ đệm cần được quan tâm. Giá trị nhập vào không mong muốn là giá trị không theo mẫu quy định có thể gây nên lỗi làm khóa (treo) tiến trình đang thực hiện hoặc cấm dịch vụ.

• Các ứng dụng WEB: các chương trình ứng dụng web hiện nay được viết khá nhanh, vì thế thường hay có lỗi trong cấu hình. Có rất nhiều báo cáo đưa ra các lỗi trong phần mềm duyệt web như lỗi trong IE, Mozzila… Dưới đây là một số ví dụ điển hình:

- Lưu giữ mật khẩu: Một rủi ro thường xảy ra khi người dùng truy nhập vào các trang WEB có yêu cầu tài khoản và mật khẩu. Thông tin này được lưu giữ tạm thời trên máy của người dùng, và có thể bị lấy cắp khi người dùng truy nhập vào trang WEB khác.

- Các thành phần máy ảo: Việc sử dụng các ứng dụng java trong trang HTML có thể gây rủi ro. Một ứng dụng java có thể được lập trình để kích hoạt các lệnh trên máy duyệt WEB và lấy trộm thông tin. Để đảm bảo an ninh hầu hết các ứng dụng java đều có chứa chữ ký điện tử để xác thực.
- Mã hóa kênh truyền SSL: Các trình duyệt hầu hết đều đảm bảo an toàn thông tin với mã hóa SSL và xác nhận chứng thực điện tử từ máy chủ gốc. Tuy nhiên các trình duyệt lại không xác nhận được các chứng thực điện tử đã hết hạn, không xác thực được các kết nối SSL được tạo ra từ cùng một máy chủ. Điều này có thể tạo ra lỗ hổng để những kẻ xâm nhập có thể lợi dụng truy nhập vào kết nối SSL và phá hủy dữ liệu.

• Ăn trộm thông tin tài khoản và mật khẩu: Hầu hết những người sử dụng mạng đều đã từng một lần thiết lập mật khẩu dễ nhớ, dựa vào tên người thân, tên tên vật… Đây là những dạng mật khẩu dễ bị phá hoặc đoán được. Dưới đây là một số hình thức ăn trộm mật khẩu:

- Lấy thông tin mật khẩu từ dữ liệu lưu trữ mật khẩu: tập tin mật khẩu (password), dữ liệu thư mục (LDAP).
- Sử dụng công cụ sniffer để tìm mật khẩu thông qua việc thu thập gói tin trên mạng.
- Thực hiện lại việc truy nhập vào mạng bằng cách mô phỏng lại những gì thu được bằng công cụ sniffer.
- Đoán mật khẩu dựa trên dữ liệu thu được.

Khiếm khuyết của giao thức

Một số bộ giao thức, ví dụ như TCP/IP, được thiết kế mà không có sự quan tâm đến vấn đề bảo mật vì thế gây ra những lỗ hổng an ninh khi áp dụng (Vấn đề này sẽ được đề cập rõ hơn trong phần tấn công mạng).

• Giao thức NFS: giao thức chia sẻ tài nguyên sử dụng trong hệ điều hành Novell và UNIX. Giao thức này không có cơ chế xác thực và mã hóa, ngoài ra NFS sử dụng cơ chế lựa chọn cổng TCP ngẫu nhiên vì thế rất khó để thiết lập điều khiển truy nhập cho hệ thống.

- Bộ giao thức TCP/IP: Bộ giao thức này chứa các giao thức như icmp, udp, tcp và một số điểm yếu khác. Ví dụ: phần mào đầu của gói tin IP có thể bị chặn và sửa đổi mà không cần để lại dấu vết. Gói tin ICMP có thể lợi dụng trong tấn công DDoS (Chúng ta sẽ bàn kỹ hơn về bộ giao thức TCP/IP trong mục các kiểu tấn công mạng).

1.3. Vấn đề an ninh trong mô hình mạng TCP/IP

1.3.1. Mô hình mạng phân lớp TCP/IP

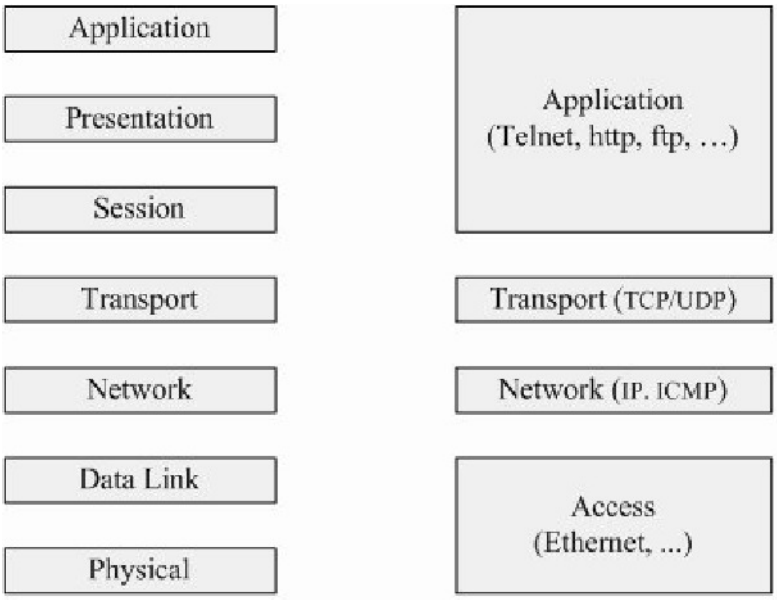
Với mục đích xây dựng một mạng máy tính mà là "mạng của các mạng", vào giữa những năm 70s Vint Cerf (Đại học Stanford) cùng Robert Kahn (BBN) đã cùng phát triển họ giao thức TCP/IP, đến năm 1983 đã thay thế hoàn toàn NCP trong ARPAnet và hiện nay TCP/IP được sử dụng phổ biến nhất trên mạng Inernet và được hỗ trợ bởi mọi phần mềm về mạng. Bởi vì TCP/IP là tên của bộ giao thức chuẩn dùng cho mạng mở và được sử dụng rộng rãi cho mạng Internet, nên nó được sử dụng như là tên của mô hình kiến trúc cho Internet về thực chất nó chỉ là hai giao thức trong mô hình.

Cũng giống như mô hình OSI mô hình TCP/IP cũng có kiến trúc phân tầng, chức năng của tầng trên được đưa ra bởi tầng dưới, mỗi giao thức có thể hoạt động độc lập với giao thức các tầng khác. Ví dụ chúng ta có thể nâng cấp hay sửa chữa giao thức của một tầng nào đó mà không sợ ảnh hưởng tới chức năng của tầng đó cũng như các tầng khác cũng như không cần phải thay đổi giao thức các tầng khác. Gần đây nhất là sự ra đời của phiên bản IP mới gọi là IPng (IP next generation hay IP version 6) được thay đổi để tạo giải pháp mới cho địa chỉ IP, sự thay đổi này không cần thay đổi kiến trúc TCP/IP và quan hệ giữa các giao thức.

- Lớp thấp nhất là lớp truy cập mạng (network access layer). Giao thức lớp này cung cấp cho hệ thống các phương thức truyền dữ liệu trên các tầng vật lí khác nhau, liên kết và định dạng dữ liệu đóng gói vào các Frame ánh xạ địa chỉ IP vào địa chỉ vật lí được dùng cho mạng.
- Lớp liên mạng hay còn gọi là lớp IP cung cấp giao thức để định nghĩa hệ thống địa chỉ liên mạng, định tuyến các gói dữ liệu phân mảnh và hợp nhất các

gói dữ liệu lớn..., đây là lớp đóng phần quan trọng nhất trong mô hình TCP/IP.

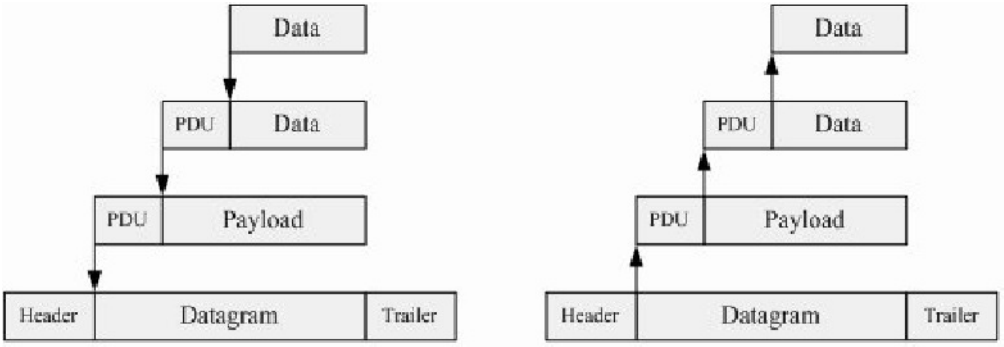
- Lớp giao vận có hai giao thức quan trọng nhất là TCP và UDP, cung cấp khả năng truyền dữ liệu một cách đáng tin cậy (TCP) hoặc thực sự đơn giản không cần kết nối hai chiều (UDP)..
- Lớp trên cùng là lớp ứng dụng nhằm cung cấp các dịch vụ đa dạng cho người dùng như Telnet, SMTP, FTP...



Hình 1.2 – Mô hình phân lớp OSI và TCP/IP

Các lớp cùng chức năng trên hai hệ thống trong mô hình trao đổi thông tin với nhau thông qua các giao thức. Một khái niệm quan trọng trong mô hình phân lớp là đóng gói dữ liệu. Quá trình đóng gói dữ liệu được thực hiện từ lớp ứng dụng xuống tới lớp vật lý tại phía phát và mở quá trình mở gói ngược lại được thực hiện phía đầu thu. Mỗi một lớp trong mô hình TCP/IP sử dụng các thông tin điều khiển của mình để có thể giao tiếp được với lớp đó tại phía thu. Những thông tin điều khiển này được thêm vào gói tin và được truyền xuống lớp dưới, quá trình này gọi là đóng gói (encapsulation). Khi gói tin được truyền từ lớp ứng dụng xuống đến mạng thông qua bảy lớp sẽ được đóng gói tại các lớp. Gói tin được chuyển đi tới nút nhận và quá trình ngược lại xảy ra. Tại các lớp của phía thu sẽ lần lợp cắt bỏ đi những

thông tin điều khiển của lớp đó cho đến khi gói tin được chuyển lên lớp ứng dụng. Quá trình như vậy gọi là mở gói (decapsulation).



Hình 1.3 – Quá trình đóng gói và mở gói

TCP/IP là họ giao thức mở chuẩn truyền thông liên mạng, có khả năng tương thích với nhiều mạng vật lí khác nhau, các tính năng của TCP/IP ngày càng được hoàn thiện và bộ giao thức này được sử dụng như một ngôn ngữ chung để nối các máy tính trên khắp thế giới với nhau.

1.3.2. An ninh mạng trong mô hình TCP/IP

An ninh tại lớp ứng dụng

An ninh tầng ứng dụng cung cấp sự bảo vệ kết nối đầu cuối từ một ứng dụng chạy trên một hệ thống thông qua mạng sang ứng dụng trên hệ thống khác. Nó không quan tâm tới cơ cấu truyền dẫn ở các lớp dưới. Tuy nhiên an ninh tại tầng ứng dụng không phải là giải pháp chung, bởi vì mỗi tầng ứng dụng cần thích ứng để đảm bảo các dịch vụ an toàn. Sau đây là một vài ví dụ của sự mở rộng an ninh tầng ứng dụng:

PGP (Pretty Good Privacy)

PGP là một chương trình phổ biến dùng trong mã hóa thư điện tử, ngoài ra nó còn dùng để gửi chữ ký điện tử đảm bảo xác nhận giữa người gửi và người nhận. Đây là một chương trình miễn phí được Philip R. Zimmermann tạo ra từ năm 1991 và hiện nay trở thành một tiêu chuẩn cho an ninh của thư điện tử.

PGP hoạt động theo nguyên tắc khi gửi thư chúng ta sử dụng khóa công khai của

người nhận để mã hóa và giải mã bằng khóa riêng. Tuy nhiên việc mã hóa và giải mã trực tiếp nội dung thư sẽ tiêu tốn nhiều thời gian, vì thế PGP sử dụng thuật toán mã hóa nhanh hơn (mã hóa đối xứng) để mã hóa nội dung và dùng mã hóa khóa công khai để mã hóa khóa mật mã. Cả nội dung đã được mã hóa và khóa mật mã đã được mã hóa đều được gửi đi trong thư. Người nhận sẽ giải mã khóa mật mã và sử dụng khóa đó để giải mã nội dung thư. PGP sử dụng RSA để mã hóa khóa và IDEA để mã hóa nội dung.

S-HTTP (Secure Hyper Text Transport Protocol)

S-http không được sử dụng rộng rãi nhưng nó được thiết kế để đảm bảo an ninh cho những ứng dụng web. S-HTTP cung cấp truyền dẫn tin cậy, xác thực, toàn vẹn. Nó mở rộng http để chứa các thẻ cho mã hóa và truyền dẫn an toàn. S-HTTP được sử dụng chủ yếu trong các ứng dụng thương mại.

An ninh tại lớp giao vận

An ninh lớp giao vận trực tiếp cung cấp an ninh giữa hai trạm, mục tiêu là được thiết kế để cung cấp liên kết tin cậy.

SSL (Secure Socket Layer) và TLS (Transport Layer Security)

SSL được phát triển bởi Nescape và hiện nay được dùng phổ biến trên Internet, đặc biệt cho những ứng dụng web có liên quan tới thẻ tín dụng. SSL cũng có thể thực hiện cùng với các ứng dụng khác như telnet, ftp, http… TLS là một giao thức mở dựa trên SSL v3.0. Hai giao thức này không hoạt động được với nhau nhưng TLS có khả năng hạ xuống SSL để tạo tính tương thích. SSL và TLS cung cấp an ninh cho một phiên TCP đơn. SSL và TLS cung cấp kết nối TCP an toàn cho các ứng dụng, qua đó mọi dữ liệu đều được đảm bảo an toàn. Cả hai ứng dụng sử dụng SSL (hoặc TLS) sử dụng cùng một khóa để mã hóa gọi là khóa phiên. Khóa phiên được mã hóa bằng thuật toán mã hóa khóa công khai và được truyền đi trong quá trình thiết lập kết nối.

SSH (Secure Shell)

SSH cung cấp khả năng đăng nhập an toàn từ xa và an ninh cho các dịch vụ

mạng. SSH ban đầu được thiết kế cung cấp chủ yếu cho sinh viên nhằm hạn chế tình trạng mật khẩu được truyền trên mạng dưới dạng đọc được. Hiện nay một số thiết bị mạng cũng đã hỗ trợ SSH để đảm bảo an ninh cho việc quản trị thiết bị từ xa. SSH có 3 thành phần chính:

- Giao thức lớp giao vận (Transport layer Protocol): Cung cấp cơ chế xác thực, bảo mật và toàn vẹn cho máy chủ, nó có thể nén luồng dữ liệu. Lớp giao vận ssh chạy phía trên cùng của lớp giao vận tcp, giao thức này dùng để trao đổi khóa, hàm mã hóa, hàm băm…
- Giao thức xác thực người dùng (User Authentication Protocol): Cung cấp khả năng xác thực mức người dùng giữa máy trạm và máy chủ.
- Giao thức kết nối (Connection Protocol): Ghép kênh một đường hầm được mã hóa (encrypted tunnel) vào một vài kênh thông tin. Hai thông tin cần trao đổi là kích thước cửa sổ và kiểu dữ liệu.

Lọc gói tin (Filtering)

Lọc gói có thể thực hiện ở các thiết bị lớp 3 để điều khiển gói tin bị chặn lại hay được chuyển tiếp. việc lọc gói dựa vào các thông tin lớp giao vận bao gồm các lựa chọn thiết lập kết nối, cổng TCP/UDP, kiểu dịch vụ…

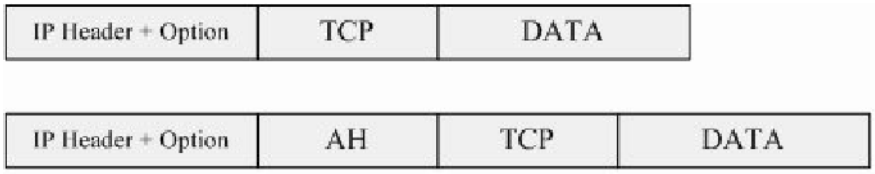
An ninh tại lớp mạng

Ipsec (Internet Protocol Security)

Cung cấp cơ chế điều khiển truy nhập, xác thực, an ninh và toàn vẹn dữ liệu cho kết nối giữa hai nút mạng (có thể là giữa hai máy chủ, hai gateway, hai máy trạm…) mà không cần có sự thay đổi về ứng dụng hoặc định tuyến.

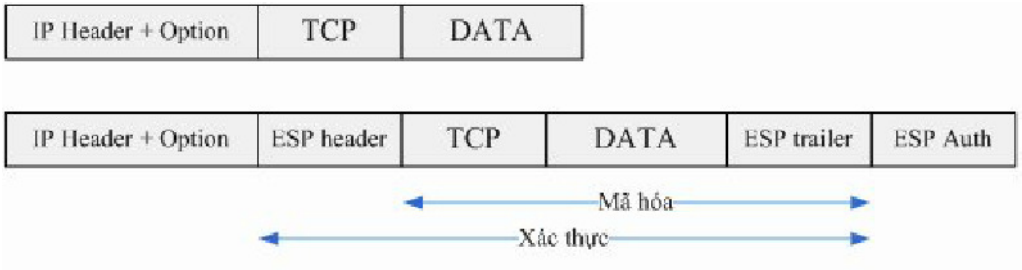
Ipsec thêm hai giao thức an ninh vào IP, gồm có:

- AH (Authentication Header): Cung cấp kết nối an toàn, xác thực dữ liệu gốc cho gói tin IP. AH không mã hóa dữ liệu nhưng bất kỳ một sự thay đổi nào trong dữ liệu gốc đều bị phát hiện.



Hình 1.4 – Gói tin IP trước và sau khi có AH

- ESP (Encapsulating Security Payload): Cung cấp sự tin cậy thông qua việc mã hóa dữ liệu. Quá trình điều khiển truy nhập được cung cấp thông qua việc quản lý các khóa để diều khiển sự tham gia vào luồng lưu lượng.



Hình 1.5 – Gói tin IP trước và sau khi có ESP

Ứng dụng chủ yếu hiện nay của Ipsec là được dùng trong các mạng riêng ảo (VPN: Virtual Private Network). VPN cho phép các trạm trên mạng có thể kết nối với nhau một cách an toàn kể cả khi sử truyền qua mạng công cộng.

Lọc gói tin (Filtering)

Lọc gói có thể thực hiện ở các thiết bị lớp 3 nhằm điều khiển cho phép hay không địa chỉ IP nguồn và đích. Các danh sách điều khiển truy nhập có thể lọc theo địa chỉ nguồn, địa chỉ đích, theo giao thức ip, icmp…

An ninh tại lớp truy nhập mạng

An ninh tại lớp truy nhập thường được thực hiện theo kiểu điểm-điểm, ví dụ như sử dụng đường kết nối trực tiếp, sử dụng frame relay. Thiết bị phần cứng đầu cuối sẽ thực hiện nhiệm vụ mã hóa và giả mã. Thông tin trên đường đi được giám sát để không bị dò rỉ. Những mạng chính phủ, mạng quân đội, ngân hàng thường sử dụng nguyên lý này để đảm bảo ninh ninh cho thông tin trên mạng.

1.4. Tấn công mạng và bảo vệ mạng

1.4.1. Sự xâm nhập mạng

Một số hoạt động có dấu hiệu chỉ ra rằng ai đó đang xâm nhập vào mạng của người khác. Mặc dù không có tài liệu nào liệt kê được nguyên nhân, lý do để ai đó thực hiện đánh cắp hay hủy dữ liệu, nhưng một lý do hiển nhiên là khi nhìn vào hoạt động xâm nhập trước đó. Để hiểu rõ hơn hoạt động xâm nhập mạng, chúng ta cần định nghĩa một số thuật ngữ. Trong khuôn khổ bài luận văn này, chúng ta coi những kẻ xâm nhập là những người tấn công để đạt lấy quyền truy nhập vào hệ thống mà không được phép. Những kẻ xâm nhập có thể được chia làm ba dạng:

- Cracker: Là những người sử dụng khả năng kiến thức về mạng, internet để tấn công an ninh một mạng máy tính mà không có quyền hạn cho phép. Cracker thường là những kẻ có ý định xấu khi xâm nhập mạng.
- Hacker: Là những người kiểm tra tính an ninh của mạng hoặc của hệ thống.dựa trên những kỹ thuật lập trình tiên tiến. Hoạt động của hacker thường không làm hại tới mạng mà chỉ là để kiểm tra tính an ninh của mạng. Những hacker có đạo đức thường là những người tư vấn an ninh cho một tổ chức hoặc công ty nào đó.
- Script kiddie: Thường là thuật ngữ để chỉ một hacker mới, còn ít kinh nghiệm và kiến thức, thường sử dụng những công cụ có sẵn trên mạng để thực hiện kiểm tra an ninh của mạng bằng phương thức dò tìm lỗ hổng của các dịch vụ.

Lý do dẫn đến hoạt động truy nhập, làm thay đổi dữ liệu hay phá vỡ mạng thường rất khác nhau. Dưới đây có thể điểm qua một vài lý do, hành động được coi là mục đích tấn công hệ thống:

- Thiếu hiểu biết về mạng máy tính: Đôi khi một người sử dụng mới, chưa có nhiều kiến thức về an ninh mạng, ví dụ những người chưa được đào tạo cơ bản về máy tính, có thể dễ dàng thay đổi dữ liệu hệ thống. Sự tin tưởng đi kèm với sự thiếu hiểu biết có thể gây nguy hiểm cho hệ thống. Một yêu cầu đối với người quản trị là không được mở toàn bộ mạng để ai đó truy nhập vào. Một người quản

trị firewall chưa được đào tạo đầy đủ có thể tạo một kết nối tới một điểm nào đó và làm cho tính an toàn của firewall trở nên kém hiệu quả.

- Xâm nhập hệ thống do hiếu kỳ: Đôi khi một ai đó xâm nhập vào hệ thống, mạng chỉ vì do tò mò, hiếu kỳ. Chẳng hạn một vụ tấn công vào hệ thống thẻ tín dụng của một ngân hàng đã xảy ra, và kẻ tấn công chỉ là một cậu bé 14 tuổi. Khi hỏi lý do vì sao, cậu ta trả lời là chỉ vì do hiếu kỳ. Hay đôi khi một số nhân viên trong một tổ chức muốn xâm nhập vào hệ thống lương chỉ để xem lương của mình và đồng nghiệp. Dữ liệu báo cáo tài chính cũng là một nguồn dữ liệu kích thích tính hiếu kỳ của các nhân viên trong tổ chức. Tùy thuộc vào sự hiếu kỳ đến mức độ nào, những sự xâm nhập không hợp pháp này có thể gây nguy hiểm ít nhiều đến mạng và hệ thống.
- Xâm nhập để vui đùa và vì phần thưởng: Nhiều người rất thích cảm giác vui sướng khi có thể vượt qua hệ thống an ninh, hệ thống an ninh càng chặt chẽ thì cảm giác đó càng lớn. Một số người lại tìm cách vượt qua hệ thống an ninh để lĩnh thưởng. Đây là nơi rất tốt để những người quản lý an ninh mạng theo dõi công nghệ mới nhất do những người này sử dụng để xâm nhập hệ thống.
- Xâm nhập để trả thù: Sự thù địch, trả thù thường dẫn đến hành động. Một số nhân viên của tổ chức có kiến thức rất tốt về mạng và biết rõ họ cần xâm nhập vào hệ thống nào để gây nên sự cố cho mạng. Vì thế một lời khuyên tốt nhất cho một tổ chức là phải luôn thay đổi mật khẩu và hủy tài khoản khi một nhân viên chủ chốt trong tổ chức rời khỏi công ty, và phải đảm bảo mạng luôn được theo dõi một cách chặt chẽ.
- Xâm nhập hệ thống vì lợi nhuận: Hệ thống thông tin thẻ tín dụng, hệ thống truyền dữ liệu không an toàn của ngân hàng luôn trở thành mục tiêu tấn công của những kẻ hám lợi. Tuy nhiên không phải mọi tấn công vì lợi nhuận đều là vì tiền. Nhiều đối thủ cạnh tranh có thể xâm nhập vào hệ thống của đối thủ khác để biết được thông tin hoạt động, báo cáo tài chính...
- Xâm nhập vì mục đích chính trị: Thực tế một nền kinh tế phụ thuộc lớn vào các giao dịch điện tử sẽ gặp rất nhiều rủi ro. Chiến tranh công nghệ và tranh chấp kinh tế sẽ xảy ra. Một nền kinh tế điện tử có thể phục thuộc vào nhiều yếu tố, trong đó

có giá thành thiết bị, giá thành kết nối, giải pháp an ninh… Năm 2002 rất nhiều hệ thống DNS đã bị tấn công với mục đích chủ yếu là làm hạn chế khả năng trao đổi thông tin giữa các tổ chức.

1.4.2. Các kiểu tấn công mạng

Trước khi thảo luận đặc điểm của những loại tấn công đặc biệt, cần phân loại những tấn công. Hành động tấn công được định nghĩa từ mục đích tấn công hơn là hành động của người tấn công. Vì thế có 3 loại tấn công chính:

- Tấn công do thám: Là loại tấn công không nhằm mục đích phá hủy lập tức hệ thống hoặc mạng nhưng đánh dấu lại mạng để phát hiện dải địa chỉ nào sử dụng, hệ thống chạy chương trình gì, thiết bị nào có trên mạng...
- Tấn công xâm nhập: Là loại tấn công khai thác lỗ hổng của mạng và chiếm quyền truy nhập vào hệ thống trên mạng. Mỗi lần truy nhập, kẻ tấn công có thể thực hiện được những việc sau:

- Thu thập, thay đổi, phá hủy dữ liệu.
- Thêm, sửa hoặc xóa tài nguyên mạng.
- Cài đặt thêm những công cụ được dùng để đạt được quyền truy nhập vào hệ thống những lần sau.

- Tấn công DoS: Là loại tấn công gây cản trở hoạt động của các hệ thống trên mạng.

Tấn công do thám

Mục đích của do thám là để thực hiện vẽ lại mạng, xác định và tìm kiếm các lỗ hổng của mạng. Một tấn công do thám có thể là một kiểu chỉ điểm cho các tấn công sau đó. Rất nhiều tấn công do thám đã được viết thành các đoạn chương trình nhỏ giúp những kẻ tấn công dễ dàng thực hiện hành động tấn công chỉ thông qua những thao tác đơn giản. Dưới đây là một số dạng tấn công:

- DNS whois: Yêu cầu dịch vụ tên miền cung cấp thông tin địa chỉ của một tên miền nào đó và chủ sở hữu tên miền đó.
- Ping sweep: đầu ra của ping sweep có thể cho chúng ta biết số máy đang hoạt động trên mạng.

- Quét chiều dọc: dùng để tìm kiếm các cổng dịch vụ từ các máy chủ, cơ chế này cho phép những người dùng không hợp pháp xác định được kiểu hệ điều hành và dịch vụ đang hoạt động.
- Quét chiều ngang: Dùng tìm kiếm dải địa chỉ đang phục vụ cho một dịch vụ nào đó. Một ví dụ là ftp sweep, đây là khả năng tìm kiếm một phân đoạn mạng có đáp ứng dịch vụ truyền tập tin trên cổng TCP 21.
- Quét khối: Là sự kết hợp của quét dọc và quét ngang. Mặt khác nó quét một phân đoạn mạng và tạo kết nối trên nhiều cổng dich vụ của một máy trên đoạn mạng.

Tấn công xâm nhập

Mục đích của tấn công là đạt được quyền truy nhập vào máy tính hoặc mạng. Để đạt được quyền truy nhập, người sử dụng cần thực hiện nhiều chức năng khác nhau. Những chức năng đó có thể được chia thành 3 loại:

- Chặn thông tin: Là khả năng bắt giữ lưu lượng mạng từ nguồn tới đích, kẻ tấn công có thể lưu giữ dữ liệu để sử dụng sau này. Dữ liệu có thể đi qua một đoạn mạng mà được nối tới một thiết bị bắt gói (sniffer), và có thể chứa những dữ liệu riêng tư như bản ghi nhân sự, tiền lương, dự án hay các thông tin quản lý mạng. Nguyên lý sử dụng cho việc chặn thông tin mạng có thể thay đổi tùy theo kiểu kết nối vật lý tới mạng. Việc nâng cấp các hệ thống hup lên switch có thể giảm được nguy bị bắt giữ của dữ liệu. Ngoài ra đối với những dữ liệu nhạy cảm, cách hiệu quả để bảo vệ là lưu dữ dưới dạng mã hóa hoặc gửi đi trên mạng dưới dạng mã hóa, điều này ngăn chặn được kẻ xâm nhập không có khả năng đọc được dữ liệu.
- Thay đổi thông tin: Khi đạt được quyền truy nhập vào hệ thống, người dùng không hợp pháp có thể làm thay đổi tài nguyên mạng. Ở đây không chỉ làm thay đổi nội dung mà còn làm thay đổi chương trình hệ thống, quyền truy nhập vào hệ thống… Quyền truy nhập không hợp lệ hoàn toàn có thể bị khai thác thành lỗ hổng trong cả hệ điều hành và các ứng dụng.
- Giả mạo thông tin: Với việc truy nhập được vào mạng, hệ thống, người dùng không hợp pháp có thể tạo ra những đối tượng lỗi và đưa vào môi trường hoạt

động của hệ thống. Điều này có thể làm thay đổi dữ liệu hoặc chèn vào hệ thống các chương trình như virus, worm hay trojan và có thể tấn công mạng, hệ thống từ những chương trình này.

- Virus: Phạm vi gây ảnh hưởng có thể từ gây khó chịu đến phá hủy hệ thống. Chúng chứa các đoạn mã có thể tự chèn vào các chương trình phần mềm. Bằng cách này mỗi lần chương trình bị nhiễm virus khởi động, chương trình virus sẽ được kích hoạt và lây lan trên máy.
- Worm: Là một loại virus khai thác lỗ hổng của mạng và có thể tự sao chép. Một chương trình worm thực hiện việc quét mạng để tìm kiếm lỗ hổng đặc biệt nào đó, khi tìm thấy, lập tức nó thực hiện sao chép tới hệ thống đó và thực hiện tiếp tục việc quét mạng từ hệ thống đó. Với cơ chế lây lan như vậy các chương trình worm có khả năng lây lan rất nhanh trên mạng.
- Trojan: Là một chương trình làm cho hệ thống khi thực hiện một chức năng này lại thực hiện một chức năng khác. Có rất nhiều kiểu trojan khác nhau và ảnh hưởng cũng rất rộng, từ gây khó chịu đến thay đổi cả cấu trúc hệ thống. Trojan đôi khi được dùng để khai thác hệ thống bằng cách tạo một tài khoản cho phép người dùng không hợp pháp có thể đạt được quyền truy nhập hoặc nâng cấp quyền của một tài khoản trên hệ thống. Một số trojan thực hiện bắt dữ liệu và gửi tới một nơi nào đó mà kẻ tấn công có thể truy nhập để thu nhận được dữ liệu đó. Một số khác cho phép kẻ tấn công có khả năng điều khiển hệ thống trong quá trình thực hiện tấn công làm ngập lụt mạng (DoS).

Tấn công ngập lụt mạng DoS

Là kiểu tấn công từ chối quyền truy nhập vào mạng. Kiểu tấn công này thường có mục tiêu vào những dịch vụ đặc biệt và tạo ra rất nhiều yêu cầu cùng một lúc tới dịch vụ đó. Nếu hệ thống không được bảo vệ sẽ không hoạt động được và bị tràn ngập bởi những yêu cầu đó. Có thể tăng số lượng rất lớn những yêu cầu như vậy bằng cách thực hiện tấn công từ nhiều hệ thống tới một hệ thống đơn, gọi là DDoS, và làm tê liệt hoạt động của mạng. DDoS thường sử dụng chương trình trojan để thực hiện tấn công.

1.4.3. Nhược điểm của bộ giao thức TCP/IP

Có lẽ khi thiết kế bộ giao thức TCP/IP người ta không quan tâm nhiều đến vấn đề an ninh mạng. Ngày nay khi mạng Internet trở nên thành công với hàng triệu máy tính, chứa một lượng dữ liệu khổng lồ, nhược điểm an ninh trong mạng TCP/IP mới được quan tâm nhiều hơn. Dưới đây là một số tấn công phổ biến khai thác lỗ hổng an ninh trong mạng TCP/IP. (Sẽ được trình bày chi tiết, cụ thể hơn ở Chương II)

Tấn công tại lớp ứng dụng

Tấn công SMTP: Cách tấn công phổ biến nhất là khai thác lỗ hổng tràn bộ đệm. Kẻ tấn công thực hiện nhập một lượng lớn ký tự vào một trường nào đó (trường địa chỉ, tiêu đề…), những ký tự nằm ngoài khả năng xư lý của chương trình cho phép kẻ tấn công có thể thực hiện một mã lệnh nào đó để xâm nhập vào hệ thống.

SMTP spam: spam hệ thống thư điện tử giống như gửi rất nhiều thư rác, thư quảng cáo gây khó chịu và làm mất thời gian của người nhận. Một vấn đề của người quản trị là thư spam tiêu tốn rất nhiều băng thông mạng, không chỉ gây cản trở hoạt động mà còn có thể làm ngừng dịch vụ giống như DoS.

Tấn công FTP: Hầu hết các máy chủ dịch vụ đều mở dịch vụ ftp mặc định và cho phép người dùng anonymous truy nhập, điều này có thể tạo ra lỗ hổng hệ thống. Những kẻ tấn công có thể truy nhập vào dịch vụ và ghi đè lên các tập tin hệ thống. Cách tốt nhất là người quản trị nên tắt dịch vụ ftp nếu không sử dụng, ngoài ra phải thường xuyên cập nhật hệ thống.

Tấn công SNMP: các dịch vụ snmp đều có từ khóa bí mật mặc định là “public” và “private”, với lệnh “snmpget” và “snmpset” kẻ tấn công có thể lấy thông tin và thay đổi cấu trúc của hệ thống. Để tránh tấn công snmp, người quản trị cần thay đổi giá trị mặc định và luôn cập nhật hệ thống.

Tấn công DNS: Dịch vụ dns là dịch vụ sống còn trong mạng, không dịch vụ nào, thậm chí cả một số thiết bị mạng, có thể hoạt động nếu thiếu DNS. Một kiểu tấn công phổ biến là tìm cách ngăn trở một máy chủ DNS trả lời yêu cầu từ một DNS thực. Ở đây các DNS cache có thể bị “đầu độc” bằng cách làm cho DNS nghĩ

cần cập nhật một bản ghi và gửi cho nó một bản ghi trống. Hậu quả là DNS sẽ không tìm thấy dữ liệu bản ghi đó cho đến khi được cập nhật lại.

Tấn công tại lớp giao vận TCP

Làm tràn TCP sync: Tấn công làm tràn TCP SYN được mô tả theo các bước sau:

- Trạm C gửi rất nhiều gói tin SYN tới trạm B từ một địa chỉ không tồn tại trên mạng.
- Trạm B gửi lại SYN/ACK và duy trì thiết lập kết nối trong hàng đợi. Hậu quả là trạm B sẽ bị hết tài nguyên để chờ ACK.
- Trạm B sẽ không có khả năng nhận được kết nối mới, dịch vụ dường như bị treo.

Hiện nay chưa có giải pháp cụ thể nào để khắc phục lỗi này. Việc ngăn ngừa chủ yếu được thực hiện trên các thiết bị mạng. Ví dụ với router của hãng cisco có thể thiết lập cấu hình TCP Intercept.

Giả mạo số TCP, đánh cắp phiên làm việc (TCP SEQ # spoofing, session hiacking): Ví dụ trạm C muốn giả trạm A để liên kết tới B:

- Trạm C thiết lập tấn công DoS tới trạm A. Mục đích là ngăn trạm A trả lời trạm B và từ đó C đóng vai trò của A.
- Trạm C thiết lập kết nối tới trạm B với địa chỉ giả là trạm A và thực hiện bắt gói tin để biết được số SEQ trong khung tin.
- Trạm B tưởng rằng đang trao đổi thông tin với trạm A (thực tế là C) và dữ liệu được chuyển đi trong phiên làm việc.

Để tránh hiện tượng này, có thể sử dụng các điều khiển truy nhập (Access Control List) trên thiết bị mạng ngăn việc giả địa chỉ từ trong ra ngoài hoặc từ ngoài vào trong, tuy nhiên không tránh được việc giả địa chỉ trong cùng một mạng.

Tấn công vào lớp mạng IP

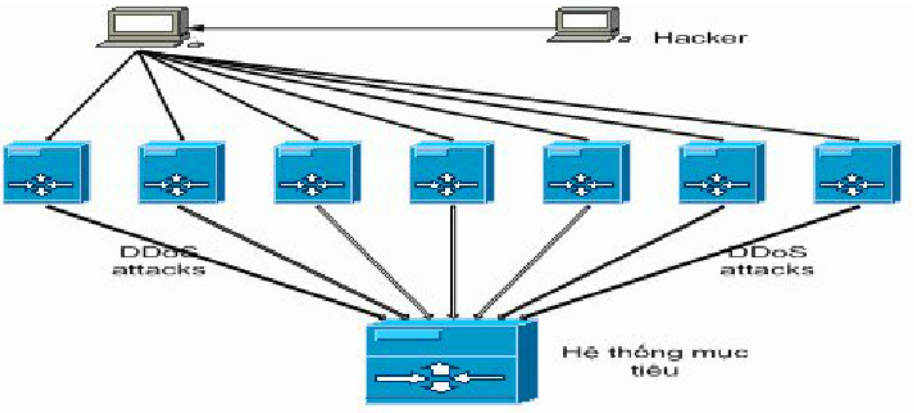
Giả mạo địa chỉ (IP spoofing): Tấn công này dựa vào việc giả mạo địa chỉ gửi tới các máy trên mạng. Ví dụ trạm C gửi quảng bá gói tin icmp trên mạng với địa chỉ nguồn là trạm A. Ngay sau đó trạm A sẽ nhận được một lượng lớn các gói tin icmp trả lời gây ảnh hưởng tới hoạt động của trạm A. Giải pháp cho vấn đề này

hiện được thực hiện trên các thiết bị mạng nhằm ngăn khả năng gửi quảng bá gói tin trên mạng, ngoài ra cũng có thể cấu hình để hệ điều hành mạng không trả lời các gói tin quảng bá.

Tấn công DoS, ping of death: Kiểu tấn công này lợi dụng lỗ hổng trong gói tin IP có chiều dài 65535 bytes. Trong tấn công này gói tin icmp được gửi đi có chiều dài lớn hơn 65535 bytes, gói tin được phân mảnh, và trạm nhận sẽ không thể thực hiện quá trình tập hợp lại được, hệ thống sẽ bị treo hoặc ngừng hoạt động.

Tấn công DoS, Teardrop: Giống như việc giả mạo IP, trạm C gửi TCP SYN tới trạm B với địa chỉ nguồn là B. Trạm B sẽ không thể thực hiện được kết nối này và xảy ra quá trình lặp, dẫn đến hệ thống bị treo.

Tấn công DoS, DDoS: Hình 1.6 miêu tả một tấn công DDoS, kẻ tấn công đạt được quyền truy nhập vào một máy trạm và thực hiện gửi lệnh tới các máy chủ. Các máy này thực hiện gửi rất nhiều gói tin tới cùng một mục tiêu. Trên thực tế có hàng ngàn máy tấn công cùng một mục tiêu với hàng tỉ gói tin làm tràn ngập toàn bộ băng thông của mạng. Vào thời điểm này chưa có giả pháp nào cho vấn đề này mà chỉ có giải pháp ngăn ngừa DDoS.



Hình 1.6 – Tấn công DDoS

1.4.4. Phương pháp bảo vệ mạng

Phương pháp điều khiển truy nhập

Điều khiển truy nhập vào hệ thống thông tin có thể được chia làm ba loại: điều khiển truy nhập ở mức vật lý, mức logic và mức quản lý. Mỗi loại này đều có hai phương thức áp dụng là ngăn ngừa và cảnh báo. Ngăn ngừa là phương pháp ngăn chặn những xâm nhập không hợp lệ vào tài nguyên hệ thống. Cảnh báo là dò tìm những xâm nhập không hợp lệ và đưa ra cảnh báo cho người quản lý hệ thống.

Ba bước để thực hiện điều khiển truy nhập là ngăn ngừa, sửa chữa, khôi phục. Ngăn ngừa là cách thức cản trở những truy nhập không hợp lệ vào tài nguyên của mạng. Sửa chữa là thực hiện những chỉnh sửa, khắc phục những lỗ hổng tồn tại trong mạng, cuối cùng là khôi phục lại hệ thống mạng, dữ liệu bị mất nếu xảy ra rủi ro.

Điều khiển truy nhập mức vật lý

Điều khiển truy nhập mức vật lý thường sử dụng các thiết bị như khóa, cổng bảo vệ, thẻ vào ra, hệ thống giám sát, cảnh báo để kiểm soát việc truy nhập vào hệ thống máy tính hay các thiết bị liên quan. Ngoài ra các hệ thống này còn để bảo vệ thiết bị khỏi các thảm họa như cháy nổ, động đất...

Điều khiển truy nhập vật lý ngăn chặn: Những giải pháp, thiết bị có nhiệm vụ ngăn chặn xâm nhập vào máy tính, các thiết bị liên quan, phòng chống các thảm họa thiên nhiên. Một số thiết bị điển hình bao gồm:

- Dữ liệu lưu trữ (backup file), các tài liệu, văn bản: Được sử dụng khi mạng gặp sự cố hư hỏng, mất dữ liệu hoặc trong trường hợp cần phục hồi cấu hình...
- Hàng rào, cổng an ninh: Những thiết bị an ninh dùng để ngăn cách vùng an ninh với các vùng khác. Nếu có sự xâm nhập vào mạng, các thiết bị này dùng để ngăn chặn và cảnh báo sự xâm nhập đó.
- Hệ thống khóa, thẻ truy nhập: Dùng để xác định quyền truy nhập của người dùng. Mỗi một người dùng được định danh bởi một mã ID gắn với thiết bị thẻ. Nhờ mã ID này, người quản trị có thể dễ dàng nhận dạng được ai đang vào vung an ninh và dễ dàng phát hiện ra người xâm nhập.
- Hệ thống phòng chống thảm họa: Các thiết bị phòng chống cháy nổ, các thiết bị chống sét, chống động đất đều rất quan trọng để ngăn ngừa ảnh hưởng của thảm

họa thiên nhiên như cháy nổ, bão, sét… có thể gây hư hỏng các thiết bị mạng, hệ thống.

Điều khiển truy nhập mức vật lý cảnh báo: Những giải pháp thiết bị có nhiệm vụ giám sát việc truy nhập vào mạng, hệ thống và đưa ra những cảnh báo cho người quản trị.

- Các thiết bị camera giám sát: Theo dõi các hoạt động trong vùng an ninh, đưa ra những cảnh báo khi có sự xâm nhập trái phép.
- Hệ thống cảnh báo cháy nổ.

Điều khiển truy nhập mức logic

Các giải pháp kỹ thuật dùng cho an ninh mạng bao gồm những giải pháp để tạo hệ thống bảo vệ cho các thiết bị phần cứng, hệ điều hành, phần mềm, các thiết bị truyền thông… Những biện pháp này còn gọi là điều khiển truy nhập ở mức logic.

Điều khiển truy nhập mức logic ngăn ngừa: Những giải pháp này chủ yếu để ngăn chặn những truy nhập trái phép từ ngoài vào trong mạng (truy nhập từ xa). Một số biện pháp sau thường được thực hiện:

- Sử dụng danh sách điều khiển (Access Control List): Sử dụng các thiết bị mạng hay phần mềm để ngăn chặn các kết nối từ xa tới một vùng tài nguyên nào đó trên mạng cần được bảo vệ.
- Sử dụng các giải pháp xác thực (Authentication): Sử dụng các giải pháp xác thực khác nhau theo từng cấp độ, đối với từng loại người dùng và theo các vùng an ninh mạng khác nhau. Các phương pháp hay sử dụng là mật khẩu, thẻ nhận dạng (token key), chứng nhận điện tử (certificate), mật khẩu một lần (one-time password)...

Điều khiển truy nhập mức logic cảnh báo: Có nhiệm vụ cảnh báo những người có ý định xâm nhập mạng hay cố tình vượt qua các hệ thống an ninh để xâm nhập mạng. Một số giải pháp cơ bản như:

- Sử dụng nhật ký mạng, hệ thống: Một nhật ký ghi lại những hoạt động của hệ

thống cho phép chúng ta có thể tái tạo lại hay kiểm tra lại toàn bộ sự kiện đã xảy ra trong một phiên làm việc từ khi có dữ liệu vào đến kết quả cuối cùng. Các dấu hiệu truy nhập hay có ý định truy nhập hệ thống có thể tìm thấy trong nhật ký mạng. Các bản ghi nhật ký phải thường xuyên được theo dõi, kiểm tra để xem xét những truy nhập thành công hay không thành công vào mạng.

- Sử dụng hệ thống dò tìm xâm nhập: Đây là một hệ thống chuyên gia, làm nhiệm vụ trích các thông tin từ phiên truy nhập của người sử dụng và kiểm tra tính xác thực của truy nhập đó. Nếu tính xác thực là không được chấp nhận thì một tín hiệu cảnh báo sẽ được chuyển đến người quản trị để đưa ra những biện pháp phòng ngừa hay ngăn chặn một cách có hiệu quả.

Điều khiển truy nhập mức quản lý

Điều khiển truy nhập mức quản lý ngăn chặn: Là một biện pháp kỹ thuật hướng con người (có sự tham gia của các nhân viên quản lý) để điều khiển các hành động của cong người đảm bảo tính tin cậy, toàn vẹn và tính sẵn sàng của dữ liệu cũng như hệ thống, bao gồm một số biện pháp sau:

- Đào tạo kỹ thuật và đào tạo an ninh.
- Phân tách trách nhiệm rõ ràng.
- Có quy trình cho những nhân viên mới và những người thôi việc.
- Có chính sách an ninh tốt và quy trình an ninh.
- Giám sát, theo dõi thường xuyên.
- Có kế hoạch khôi phục sau thảm họa.
- Có bản đăng ký truy nhập vào mạng, hệ thống.

Điều khiển truy nhập mức quản lý dò tìm: Dùng để xác định việc thực hiện chính sách an ninh trong mạng, tìm lỗi và tránh để những nhân viên trong tổ chức gây ra những rủi ro cho mạng. Một số giải pháp bao gồm:

- Kiểm tra và ghi lại sự kiện an ninh
- Ước lượng công việc, hiệu suất.
- Thanh tra, kiểm tra tổng thể.
- Quay vòng trách nhiệm.

Phương pháp mã hóa thông tin

Mã hóa là khoa học của viết và đọc trong vấn đề mật mã. An toàn thông tin sử dụng hệ thống mã hóa để giữ thông tin mang tính chất riêng tư, đồng thời xác thực đích danh người nhận và người gửi. Mã hóa có thể cung cấp những tính năng ưu việt bởi nó không chỉ cho phép xác thực người hay tiến trình truy nhập mà còn cho phép nhận biết được sự thay đổi hay phá hỏng thông tin gốc. Mã hóa được thực hiện bằng cách thêm dữ liệu hoặc kéo dãn xung nhịp.

Có ba kiểu mã hóa thường sử dụng là mã hóa đối xứng, mã hóa bất đối xứng và hàm băm (hash function). Hầu hết các thuật toán mã hóa đều được công bố rộng rãi và đã được các chuyên gia thử nghiệm về tính an toàn của nó. Tính bảo mật chỉ phụ thuộc vào độ dài của hàm mã hóa và độ dài từ khóa.

Có rất nhiều nguyên lý mã hóa thông tin. Để truyền một bản tin đã mật mã, những bên tham gia phải sử dụng cùng một nguyên lý mã hóa và sử dụng cùng một khóa mã hóa. Dưới đây là một số phương pháp mã hóa phổ biến được sử dụng trên mạng.

Mã hóa đối xứng

Mã hóa đối xứng sử dụng cùng một khóa mã để mã hóa thông tin và giải mã. Mỗi cặp người dùng chia sẻ cùng một khóa mã cho việc trao dổi thông tin. Với kiểu mã hóa này, khóa mã phải được giữ bí mật giữa hai người trao đổi thông tin với nhau. Có một số hàm sau sử dụng cho mã hóa đối xứng.

- DES (Data Encryption Standard): Sử dụng khóa mã hóa 56-bit mã hóa cho từng khối dữ liệu 64-bit. 3DES sử dụng khóa mã 168-bit.
- IDEA (International Data Encryption Agorithm): Sử dụng khóa mã 128-bit, sử dụng phương thức mã hóa khối (block cipher).
- RC4 (Rivest Cipher 4): Sử dụng phương thức mã hóa dòng (stream cipher) với chiều dài từ khóa có thể thay đổi.
- AES (Advanced Encryption Standard): Sử dụng phương pháp mã hóa khối (block cipher) 128-bit, hỗ trợ các khóa mã 128-bit, 192-bit và 256-bit.

Mã hóa bất đối xứng

Mã hóa bất đối xứng được biết đến nhiều hơn với tên là mã hóa khóa công khai (public key cryptography). Nó sử dụng một cặp khóa có quan hệ về mặt toán học. Một khóa dùng để mã hóa, một khóa để giải mã. Một khóa được giữ bí mật, một khóa công khai. Nguyên lý của mã hóa bất đối xứng là hàm mã hóa lật một chiều. Có thể dễ dàng tính theo một chiều nhưng khó tính được theo chiều ngược lại, trừ khi có được thông tin lật (trapdoor). Một số hàm sau được sử dụng cho mã hóa bất đối xứng.

- Diffie-Hellman
- RSA (Rivest, Shamir, Adleman)
- DSA Digital Signature Algorithm)
- ECC (Elliptic Curve Cryptosystem)

Hàm băm (Hash function)

Hàm băm thường được dùng để làm ngắn gọn một bản tin dài thành một đoạn mã có chiều dài xác định. Các thuật toán khác nhau tạo ra đoạn mã có chiều dài khác nhau. Hàm băm là cách thức mã hóa dùng để kiểm tra tính toàn vẹn của dữ liệu. một thay đổi nhỏ cũng làm thay đổi luồng bit dữ liệu và tạo ra đoạn mã khác. Hàm băm là hàm mã hóa một chiều và không thể tính ngược lại được. Một số hàm sau được dùng cho hàm băm.

- MD5 (Message Digest 5): 128 bit chiều dài từ mã.
- SHA-1 (Secure Hash Algorithm-1): 160 bit chiều dài từ mã.
- Haval: Chiều dài từ mã thay đổi

CHƯƠNG II: CÁC PHƯƠNG THỨC TẤN CÔNG VÀ CÁCH PHÒNG CHỐNG

2.1 Địa chỉ MAC

Địa chỉ MAC (Media Access Control) : là kiểu địa chỉ vật lí, đặc trưng cho một thiết bị hoặc một nhóm các thiết bị trong LAN. Địa chỉ này được dùng để nhận diện các thiết bị giúp cho các gói tin lớp 2 có thể đến đúng đích.

Một địa chỉ MAC bao gồm 6 byte và thường được viết dưới dạng hexa, với các thiết bị của Cisco, địa chỉ này được viết dưới dạng số hexa ,ví dụ: 0000.0C12.FFFF là một địa chỉ MAC hợp lệ. Để đảm bảo địa chỉ MAC của một thiết bị là duy nhất, các nhà sản xuất cần phải ghi địa chỉ đó lên ROM của thiết bị phần cứng và định danh của nhà sản xuất sẽ được xác định bởi 3 byte đầu OUI (Organizationally Unique Identifier).

Địa chỉ MAC được phân làm 3 loại

- Unicast: đây là loại địa chỉ dùng để đại diện cho một thiết bị duy nhất.

- Multicast: đây là loại địa chỉ đại diện cho một nhóm các thiết bị trong LAN. Địa chỉ được dùng trong trường hợp một ứng dụng có thể muốn trao đổi với một nhóm các thiết bị. Bằng cách gửi đi một bản tin có địa chỉ multicast; tất cả các thiết bị trong nhóm đều nhận và xử lí gói tin trong khi các thiết bị còn lại trong mạng sẽ bỏ qua. Giao thức IP cũng hỗ trợ truyền multicast. Khi một gói tin IP multicast được truyền qua một LAN, địa chỉ MAC multicast tương ứng với địa chỉ IP sẽ là 0100.5exxx.xxxx.

- Broadcast: địa chỉ này đại diện cho tất cả các thiết bị trong cùng một LAN. Điều đó cũng có nghĩa là nếu một gói tin có địa chỉ MAC là FFFF.FFFF.FFFF được gửi đi thì tất cả các thiết bị trong LAN đều phải thu nhận và xử lí.

2.2 Giới thiệu giao thức ARP

Mỗi thiết bị trong hệ thống mạng của chúng ta có ít nhất hai địa chỉ. Một địa chỉ là Media Access Control (MAC) và một địa chỉ Internet Protocol (IP). Địa chỉ MAC là địa chỉ của card mạng gắn vào bên trong thiết bị, nó là duy nhất và không hề thay đổi. Địa chỉ IP có thể thay đổi theo người sử dụng tùy vào môi trường mạng. ARP là một trong những giao thức của IP, chức năng của nó dùng để định vị một host trong một phân đoạn mạng bằng cách phân giải địa chỉ IP ra địa chỉ MAC. ARP thực hiện phân giải địa chỉ thông qua một tiến trình broadcast gói tin đến tất cả các host trong mạng, gói tin đó chứa địa chỉ IP của host cần giao tiếp. Các host trong mạng đều nhận được gói tin đó và chỉ duy nhất host nào có địa chỉ IP trùng với địa chỉ IP trong gói tin mới trả lời lại, còn lại sẽ tự động drop gói tin.ARP là một giao thức hết sức đơn giản, nó đơn thuần có 4 loại message cơ bản sau:

- An ARP Request: máy tính A sẽ hỏi toàn mạng : " Ai có địa chỉ IP này? "
- An ARP Reply: máy tính B trả lời máy tính A : "Tôi có IP đó, địa chỉ MAC của tôi là..."
- An Reverse ARP Request: máy tính A sẽ hỏi toàn mạng : " Ai có địa chỉ MAC này? "
- An Reverse ARP Reply: máy tính B trả lời máy tính A: " Tôi có MAC đó, địa chỉ IP của tôi là..."

Host A gửi một ARP Request và nhận được một ARP Reply từ một host B có thực trong mạng. Sau khi tiến trình này hoàn tất, host A biết host B sẽ có MAC như thế nào. Tiếp theo, host A sẽ lưu lại sự hiểu biết đó lên bộ nhớ của mình gọi là ARP table. ARP table giúp host A không phải thực hiện ARP Request đến host B một lần nữa.

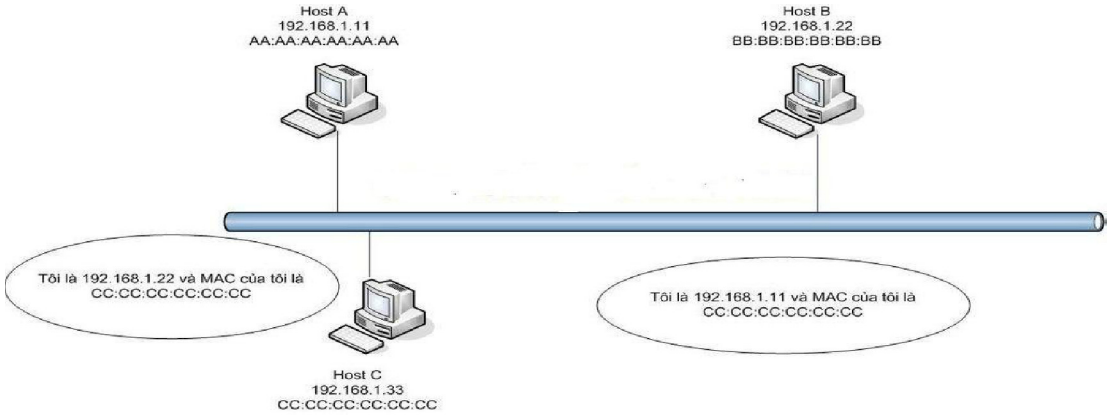
Mô tả quá trình ARP Request và ARP Reply trong LAN:

Trong LAN hiện nay có 4 host: host A, host B, host C, host D.

- Host A muốn giao tiếp với host C, đầu tiên sẽ broadcast gói tin ARP Requset.

- Host C nhận thấy đúng IP của mình liền trả lời MAC của mình thông qua gói tin ARP Reply, các host còn lại sẽ drop gói ARP Request.

- Host A nhận được địa chỉ MAC của host C và ghi nhớ vào ARP table.



Hinh 2.1 – Quá trinh ARP Request va ARP Reply trong LAN

2.3 Mô tả quá trình ARP Request và ARP Reply trong môi trương hê thông mang

Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C.

Host A thuộc mạng A muốn gửi gói tin đến host B thuộc mạng B. Do các broadcast không thể truyền qua Router nên khi đó host A sẽ xem Router C như một cầu nối hay một trung gian (Agent) để truyền dữ liệu.

Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (routing table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của

Router C. Bảng định tuyến sẽ có chứa địa chỉ IP của port X. Quá trình truyền dữ liệu theo từng bước sau :

- Host A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.
- Router C trả lời, cung cấp cho host A địa chỉ MAC của port X.
- Host A truyền gói tin đến port X của Router.
- Router nhận được gói tin từ host A, chuyển gói tin ra port X của Router. Trong gói tin có chứa địa chỉ IP của host B. Router sẽ gửi ARP request để tìm địa chỉ MAC của host B.
- Host B sẽ trả lời cho Router biết địa chỉ MAC của mình. Sau khi nhận được địa chỉ MAC của host B, Router C gửi gói tin của A đến B.

Trên thực tế ngoài dạng bảng định tuyến này người ta còn dùng phương pháp proxyARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác.Theo đó các máy trạm không cần giữ bảng định tuyến nữa Router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy.

2.4 Các dạng tấn công dựa trên giao thức ARP:

Giao thức ARP là rất cần thiết và quan trọng trong hệ thống mạng, tuy nhiên giao thức này không có tính năng xác thực nào cả. Khi một host nhận được gói tin ARP Reply, nó hoàn toàn tin tưởng và mặc nhiên sử dụng thông tin đó để sử dụng sau này mà không cần biết thông tin đó có phải trả lời từ một host mà mình mong muốn hay không. ARP không có cơ chế nào để kiểm tra việc này và trên thực tế một host có thể chấp nhận gói ARP Reply mà trước đó không cần phải gửi gói tin ARP Request. Lợi dụng điều này, hacker có thể triển khai các phương thức tấn công như: Man In The Middle, Denial of Service, MAC Flooding.

2.4.1 Man in the Middle:

Giả sử hacker muốn theo dõi host A gởi thông tin gì cho host B. Đầu tiên, hacker sẽ gởi gói ARP Reply đến host A với nội dung là địa chỉ MAC của hacker và địa chỉ IP của hostB.

Tiếp theo, hacker sẽ gửi gói ARP Reply tới host B với nội dung là MAC của máy hacker và IP của host A. Như vậy, cả hai host A và host B đều tiếp nhận gói ARP Reply đó và lưu vào trong ARP table của mình. Đến lúc này, khi host A muốn gửi thông tin đến host B, nó liền tra vào ARP table thấy đã có sẵn thông tin về địa chỉ MAC của host B nên sẽ lấy thông tin đó ra sử dụng, nhưng thực chất địa chỉ MAC đó là của hacker. Đồng thời máy tính của hacker sẽ mở chức năng gọi là IP Forwading giúp chuyển tải nội dung mà host A gửi qua host B. Host A và host B giao tiếp bình thường và không có cảm giác bị qua máy trung gian là máy của hacker.Trong trường hợp khác, hacker sẽ nghe lén thông tin từ máy bạn đến Gateway. Như vậy mọi hành động ra Internet của bạn đều bị hacker ghi lại hết, dẫn đến việc mất mát các thông tin nhạy cảm. Môt sô dang tân công sư dung ky thuât Man in the Middle : ARP Cache, DNS Spoofing, Hijacking HTTP session.

ARP Cache (ARP Poison Routing):

- **ARP Cache**

ARP co thê coi như môt bang chưa môt tâp tương ưng giưa cac phân cưng va cac đia chi IP. Môi thiêt bi trên mang đêu co cache riêng. Đê qua trinh phân giai đia chi diên ra nhanh ta co thê sư dung cac cach sau đê lưu giư cac entry trong cache:

- Sư dung ARP cache tinh :Môi đia chi IP va đia chi MAC tương ưng đươc thêm môt cach thu công vao bang cache va đươc duy tri lâu dai.

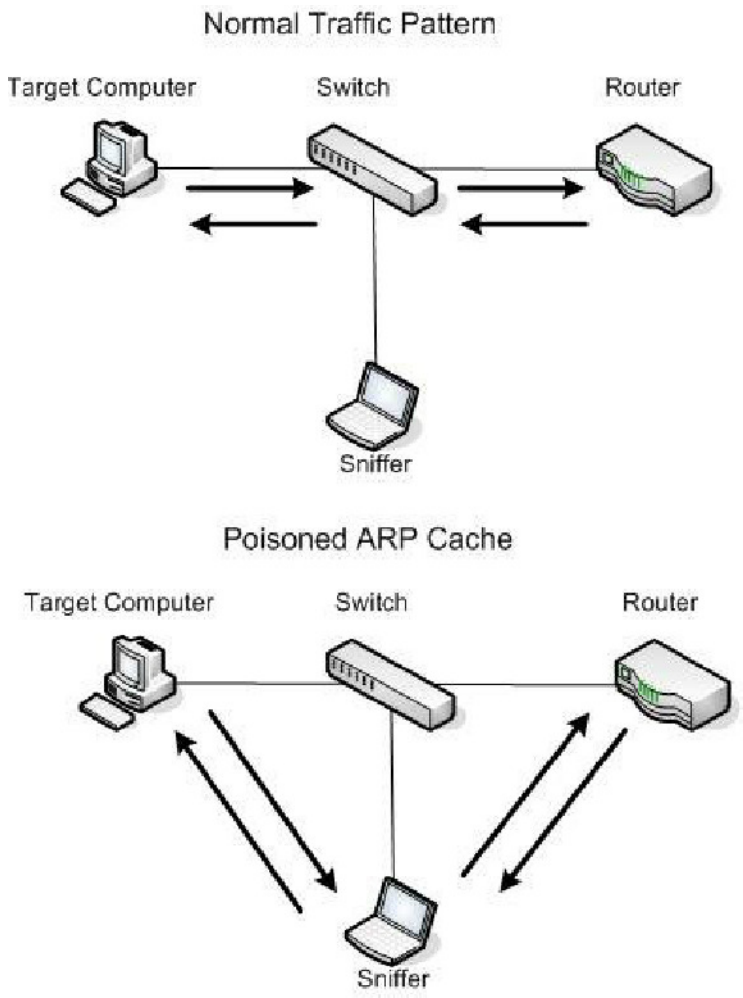
- Sư dung ARP cache đông :Đia chi IP va phân cưng đươc lưu trong cache băng phân mêm.Cac đia chi nay đươc lưu giư tam thơi va sau đo đươc gơ bo.

ARP Cache biến một quá trình có thể gây lãng phí về mặt thời gian thành một quá trình sử dụng thời gian một cách hiệu quả. Mặc dù vậy nó có thể bắt gặp một số vấn đề như : cần phải duy trì bảng cache, thêm vào đó cũng có thể các entry cache bị "cũ" theo thời gian, vì vậy cần phải thực thi hết hiệu lực đối với các entry cache sau một quãng thời gian nào đó.

- **Nguyên ly tân công:**

Phương phap tấn công này cho phép kẻ tấn công (nằm trên cùng một subnet với các nạn nhân của nó) có thể nghe trộm tất cả các lưu lượng mạng giữa các máy tính nạn nhân. Đây là một trong những hình thức tấn công đơn giản nhất nhưng hiêu qua.

Việc giả mạo bảng ARP chính là lợi dụng bản tính không an toàn của giao thức ARP. Không giống như các giao thức khác, chẳng hạn như DNS (có thể được cấu hình để chỉ chấp nhận các câp nhât động khá an toàn), các thiết bị sử dụng giao thức phân giải địa chỉ (ARP) sẽ chấp nhận câp nhât bất cứ lúc nào. Điều này có nghĩa rằng bất cứ thiết bị nào cung có thể gửi gói ARP reply đến một máy tính khác và máy tính này sẽ cập nhật vào bảng ARP cache của nó ngay giá trị mới này. Việc gửi một gói ARP reply khi không có request nào được tạo ra được gọi là việc gửi ARP "vu vơ". Khi các ARP reply vu vơ này đến được các máy tính đã gửi request, máy tính request này sẽ nghĩ rằng đó chính là đối tượng mình đang tìm kiếm để truyền thông, tuy nhiên thực chất họ lại đang truyền thông với một kẻ tấn công.



Hinh 2.2 – Chặn băt thông tin băng cach gia mao ARP cache.

Đê thưc hiên phương phap tân công nay ta co thê sư dung môt sô công cu như Cain & Abel , Wireshark.

- **Phương pháp phòng chống:**

Phong chông tân công ARP cache găp môt sô bât lơi vi quá trình ARP xảy ra trong chế độ background nên có rất ít khả năng có thể điều khiển trực tiếp được chúng. Không có một giải pháp cụ thể nào đê phong thu hưu hiêu nhưng tuy tinh huông ta co thê sư dung môt sô phương phap sau:

- **Ma hoa ARP cache**

Một cách có thể bảo vệ chống lại vấn đề không an toàn vốn có trong các ARP request và ARP reply là thực hiện một quá trình kém động hơn. Đây là một tùy

chọn vì các máy tính Windows cho phép bạn có thể bổ sung các entry tĩnh vào ARP cache. Ta có thể xem ARP cache của máy tính Windows bằng cách mở cmd và đánh vào đó lệnh arp –a.

Có thể thêm các entry vào danh sách này bằng cách sử dụng lệnh : arp –s <IP ADDRESS> <MAC ADDRESS>.

Trong các trường hợp, cấu hình mạng it co sư thay đổi, ta có thể tạo một danh sách các entry ARP tĩnh và sử dụng chúng cho các client thông qua một kịch bản tự động. Điều này sẽ bảo đảm được các thiết bị sẽ luôn dựa vào ARP cache nội bộ của chúng thay vì các ARP request và ARP reply.

- Kiêm tra lưu lương ARP cache vơi chương trinh cua hang thư 3:

Môt biên phap phòng chống lại viêc giả mạo ARP cache là phương pháp kiểm tra lưu lượng mạng của các thiết bị. Ta có thể thực hiện điều này với một vài hệ thống phát hiện xâm phạm (chẳng hạn như Snort) hoặc thông qua các tiện ích được thiết kế đặc biệt cho mục đích này (như xARP). Điều này có thể khả thi khi ta chỉ quan tâm đến một thiết bị nào đó, tuy nhiên nó vẫn khá cồng kềnh và vướng mắc trong việc giải quyết với toàn bộ phân đoạn mạng.

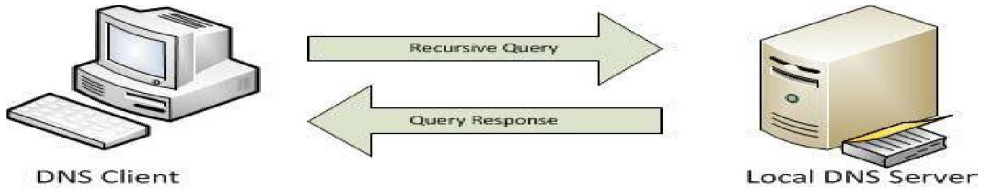
a. Gia mao DNS (DNS Spoofing):

- **Truyên thông DNS:**

Giao thức Domain Naming System (DNS) được định nghĩa trong RFC 1034/1035 có thể được xem như là một trong những giao thức quan trọng nhất được sử dụng trong Internet. Nói ngắn ngọn để dễ hiểu, bất cứ khi nào ta đánh một địa chỉ web chẳng hạn như http://www.google.com vào trình duyệt, yêu cầu DNS sẽ được đưa đến máy chủ DNS để tìm ra địa chỉ IP tương xứng với tên miền mà ta vừa nhập. Các router và các thiết bị kết nối Internet sẽ không hiểu google.com là gì, chúng chỉ hiểu các địa chỉ chẳng hạn như 74.125.95.103.

Máy chủ DNS làm việc bằng cách lưu một cơ sở dữ liệu các entry (được gọi là bản ghi tài nguyên) địa chỉ IP để bản đồ hóa tên DNS, truyền thông các bản ghi tài nguyên đó đến máy khách và đến máy chủ DNS khác. Ơ đây ta sẽ không đi

vào giới thiệu các khía cạnh về kiến trúc hay thậm chí các kiểu lưu lượng DNS khác nhau, mà chỉ giới thiệu một phiên giao dịch DNS cơ bản.



Hình 2.3:Truy vấn và hồi đáp DNS

DNS hoạt động theo hình thức truy vấn và đáp trả (query/response). Một máy khách cần phân giải DNS cho một địa chỉ IP nào đó sẽ gửi đi một truy vấn đến máy chủ DNS, máy chủ DNS này sẽ gửi thông tin được yêu cầu trong gói đáp trả của nó. Đứng ở góc độ máy khách , chỉ có hai gói xuất hiện lúc này là truy vấn và đáp trả.

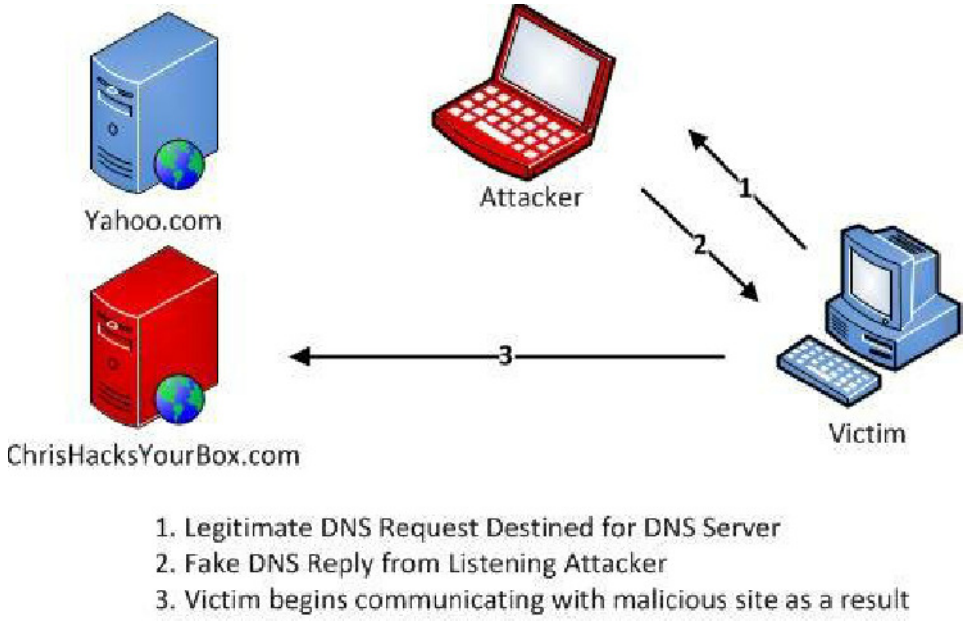
Hình 2.4: Truy vấn và hồi đáp DNS bằng đệ quy

- **Nguyên lý giả mạo DNS:**

Có nhiều cách để có thể thực hiện vấn đề giả mạo DNS. Ở đây ta sẽ tìm hiểu kỹ thuật giả mạo DNS ID.

Mỗi truy vấn DNS được gửi qua mạng đều có chứa một số nhận dạng duy nhất, mục đích của số nhận dạng này là để phân biệt các truy vấn và đáp trả chúng. Điều này có nghĩa rằng nếu một máy tính đang tấn công của chúng ta có thể chặn một truy vấn DNS nào đó được gửi đi từ một thiết bị cụ thể, thì tất cả những gì chúng ta cần thực hiện là tạo một gói giả mạo có chứa số nhận dạng đó để gói dữ liệu đó được chấp nhận bởi mục tiêu.

Chúng ta sẽ hoàn tất quá trình này bằng cách thực hiện hai bước với một công cụ đơn giản. Đầu tiên, chúng ta cần giả mạo ARP cache thiết bị mục tiêu để định tuyến lại lưu lượng của nó qua host đang tấn công của mình, từ đó có thể chặn yêu cầu DNS và gửi đi gói dữ liệu giả mạo. Mục đích của kịch bản này là lừa người dùng trong mạng mục tiêu truy cập vào website độc thay vì website mà họ đang cố gắng truy cập



Hình 2.5 – Tấn công giả mạo DNS bằng cách giả mạo DNS ID

Có thể sử dụng công cụ Ettercap để thực hiện mô phỏng tấn công giả mạo DNS.

- **Phòng chống tấn công giả mạo DNS:**

Việc phòng thủ với tấn công giả mạo DNS khá khó khăn vì có ít các dấu hiệu để nhận biết bị tấn công. Thông thường, ta không hề biết DNS của mình bị giả mạo cho tới khi điều đó xảy ra. Kết quả nhận được là một trang web khác hoàn toàn so với những gì mong đợi. Trong các tấn công với chủ đích lớn, rất có thể người dùng sẽ không hề biết rằng mình đã bị lừa nhập các thông tin quan trọng của mình vào một website giả mạo. Sau đây là một số phương pháp phòng thủ tấn công giả mạo DNS:

- Bảo vệ các máy tính bên trong của mạng: Các tấn công giống như trên thường được thực thi từ bên trong mạng . Nếu các thiết bị mạng an toàn thì ta sẽ giảm được khả năng các host bị thỏa hiệp và được sử dụng để khởi chạy tấn công giả mạo.

- Không dựa vào DNS cho các hệ thống bảo mật: Trên các hệ thống an toàn và có độ nhạy cảm cao, không duyệt Internet trên nó là cách thực hiện tốt nhất để không sử dụng đến DNS. Nếu dùng phần mềm sử dụng hostname để thực hiện một số công việc của nó thì chúng cần phải được điều chỉnh cho phù hợp trong file cấu hình thiết bị.

- Sử dụng IDS: Một hệ thống phát hiện xâm nhập, khi được đặt và triển khai đúng, có thể vạch mặt các hình thức giả mạo ARP cache và giả mạo DNS.

- Sử dụng DNSSEC: DNSSEC là một giải pháp thay thế mới cho DNS, sử dụng các bản ghi DNS có chữ ký để bảo đảm sự hợp lệ hóa của đáp trả truy vấn. Tuy DNSSEC vẫn chưa được triển khải rộng rãi nhưng nó đã được chấp thuận là "tương lai của DNS".

- **Kết luận:**

Giả mạo DNS là một hình thức tấn công MITM khá nguy hiểm khi được đi sử dụng với mục đích ăn cắp thông tin. Sử dụng công nghệ này những kẻ tấn công có thể tận dụng các kỹ thuật giả mạo để đánh cắp các thông tin quan trọng của người dùng, hay cài đặt malware trên một ổ đĩa bị khai thác, hoặc gây ra một tấn công từ chối dịch vụ.

2.4.2 Denial of Service (DOS) :

Một cuộc tấn công từ chối dịch vụ (tấn công DoS) hay tấn công từ chối dịch vụ phân tán (tấn công DDoS) là quá trình làm cho tài nguyên của một máy tính không thể sử dụng được nhằm vào những người dùng của nó. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ là khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để chống lại Internet site hoặc service (dịch vụ Web) vận hành hiệu

quả hoặc trong tất cả, tạm thời hay một cách không xác định. Thủ phạm tấn công từ chối dịch vụ nhằm vào các mục tiêu site hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

Một phương thức tấn công phổ biến kéo theo sự bão hoà máy mục tiêu với các yêu cầu liên lạc bên ngoài, đến mức nó không thể đáp ứng giao thông hợp pháp, hoặc đáp ứng quá chậm. Trong điều kiện chung, các cuộc tấn công DoS được bổ sung bởi ép máy mục tiêu khởi động lại hoặc tiêu thụ hết tài nguyên của nó đến mức nó không cung cấp dịch vụ, hoặc làm tắc nghẽn liên lạc giữa người sử dụng và nạn nhân.

- **Nhận diện:**

Dấu hiệu của một cuộc tấn công từ chối dịch vụ gồm có:

- Mạng thực thi chậm khác thường (mở file hay truy cập Website).
- Không thể dùng một Website cụ thể.
- Không thể truy cập bất kỳ Website nào.
- Tăng lượng thư rác nhận được.

Tấn công từ chối dịch cũng có thể dẫn tới vấn đề về nhánh mạng của máy đang bị tấn công. Ví dụ băng thông của router giữa Internet và Lan có thể bị tiêu thụ bởi tấn công, làm tổn hại không chỉ máy tính ý định tấn công mà còn là toàn thể mạng.

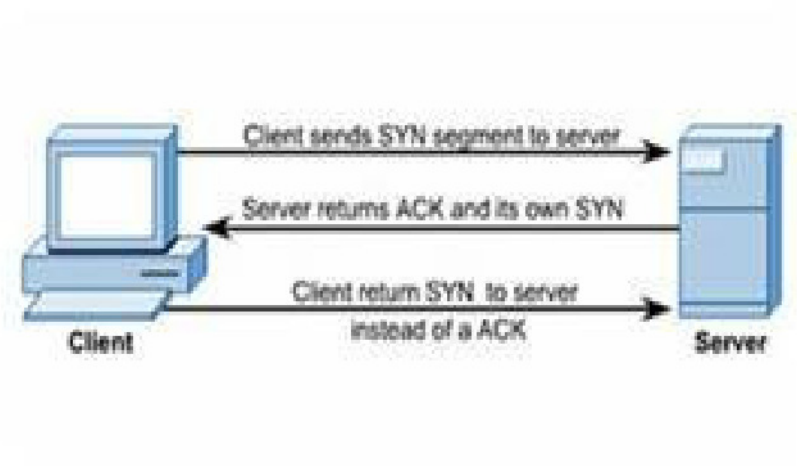
- **Các cách thức tấn công DoS:**

- Phá hoại dựa trên tính giới hạn hoặc không thể phục hồi của tài nguyên mạng:

∗ Thông qua kết nối: Kiểu tấn công SYN flood

Lợi dụng cách thức hoạt động của kết nối TCP/IP, hacker bắt đầu quá trình thiết lập một kết nối TPC/IP tới mục tiêu muốn tấn công mà không gửi trả gói tin ACK, khiến cho mục tiêu luôn rơi vào trạng thái chờ (đợi gói tin ACK từ phía yêu cầu thiết lập kết nối) và liên tục gửi gói tin SYN ACK để thiết lập kết nối.

Một cách khác là giả mạo địa chỉ IP nguồn của gói tin yêu cầu thiết lập kết nối SYN và cũng như trường hợp trên, máy tính đích cũng rơi vào trạng thái chờ vì các gói tin SYN ACK không thể đi đến đích do địa chỉ IP nguồn là không có thật. Kiểu tấn công SYN flood được các hacker áp dụng để tấn công một hệ thống mạng có băng thông lớn hơn hệ thống của hacker.



Hình 2. 6 – Kiểu tấn công SYN flood

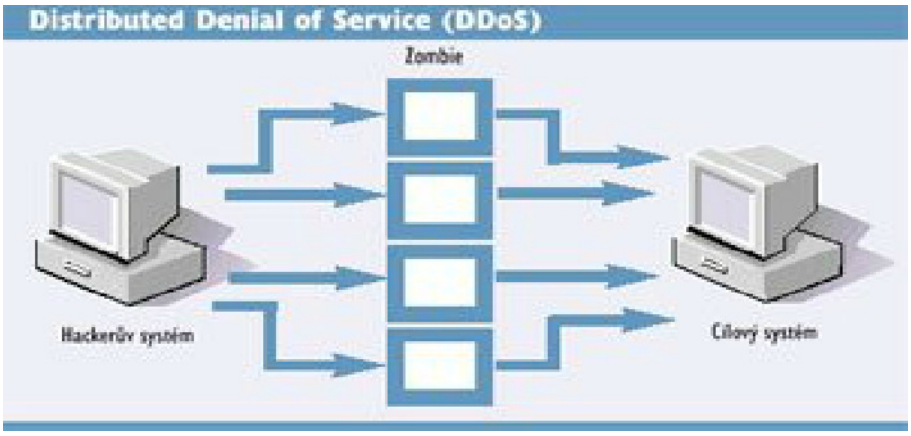
∗ Lợi dụng nguồn tài nguyên của chính nạn nhân để tấn công:

Kiểu tấn công Land Attack: Kiểu tấn công Land Attack cũng tương tự như SYN flood, nhưng hacker sử dụng chính IP của mục tiêu cần tấn công để dùng làm địa chỉ IP nguồn trong gói tin, đẩy mục tiêu vào một vòng lặp vô tận khi cố gắng thiết lập kết nối với chính nó.

Kiểu tấn công UDP flood: Hacker gửi gói tin UDP echo với địa chỉ IP nguồn là cổng loopback của chính mục tiêu cần tấn công hoặc của một máy tính trong cùng mạng. Với mục tiêu sử dụng cổng UDP echo (port 7) để thiết lập việc gửi và nhận các gói tin echo trên 2 máy tính (hoặc giữa mục tiêu với chính nó nếu mục tiêu có cấu hình cổng loopback), khiến cho 2 máy tính này dần dần sử dụng hết băng thông của chúng, và cản trở hoạt động chia sẻ tài nguyên mạng của các máy tính khác trong mạng.

∗ Sử dụng băng thông: Tấn công kiểu DDoS (Distributed Denial of Service)

Đây là cách thức tấn công rất nguy hiểm. Hacker xâm nhập vào các hệ thống máy tính, cài đặt các chương trình điều khiển từ xa, và sẽ kích hoạt đồng thời các chương trình này vào cùng một thời điểm để đồng loạt tấn công vào một mục tiêu. Với DDoS, các hacker có thể huy động tới hàng trăm thậm chí hàng ngàn máy tính cùng tham gia tấn công cùng một thời điểm (tùy vào sự chuẩn bị trước đó của hacker) và có thể "ngốn" hết băng thông của mục tiêu trong nháy mắt.

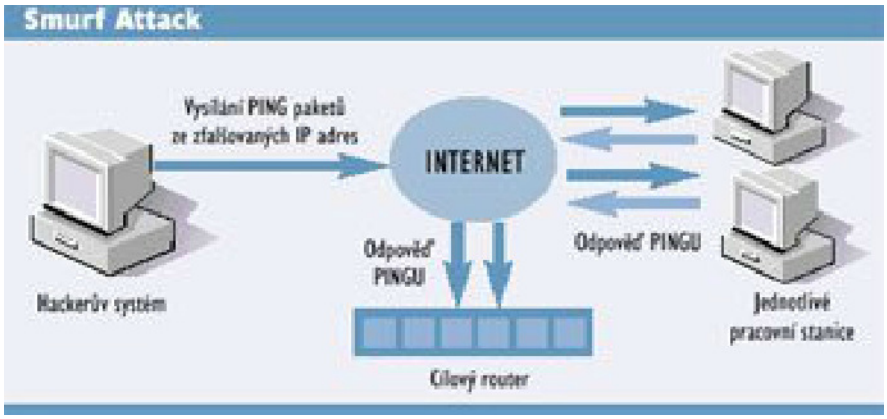


Hình 2.7 – Kiểu tấn công DDoS

∗ Sử dụng các nguồn tài nguyên khác:

Kẻ tấn công lợi dụng các nguồn tài nguyên mà nạn nhân cần đến để tấn công. Những kẻ tấn công có thể thay đổi dữ liệu và tự sao chép dữ liệu mà nạn nhân cần lên nhiều lần làm CPU bị quá tải và các quá trình xử lý dữ liệu bị đình trệ.

Tấn công kiểu Smurf Attack: Kiểu tấn công này cần một hệ thống rất quan trọng, đó là mạng khuyếch đại. Hacker dùng địa chỉ của máy tính cần tấn công bằng cách gửi gói tin ICMP echo cho toàn bộ mạng (broadcast). Các máy tính trong mạng sẽ đồng loạt gửi gói tin ICMP reply cho máy tính mà hacker muốn tấn công. Kết quả là máy tính này sẽ không thể xử lý kịp thời một lượng lớn thông tin và dẫn tới bị treo máy.



Hình 2.8 – Kiểu tấn công Smurf Attack

Tấn công kiểu Tear Drop: Trong mạng chuyển mạch gói, dữ liệu được chia thành nhiều gói tin nhỏ, mỗi gói tin có một giá trị offset riêng và có thể truyền đi theo nhiều con đường khác nhau để tới đích. Tại đích, nhờ vào giá trị offset của từng gói tin mà dữ liệu lại được kết hợp lại như ban đầu. Lợi dụng điều này, hacker có thể tạo ra nhiều gói tin có giá trị offset trùng lặp nhau gửi đến mục tiêu muốn tấn công. Kết quả là máy tính đích không thể sắp xếp được những gói tin này và dẫn tới bị treo máy vì bị "vắt kiệt" khả năng xử lý.

- ***Phá hoại hoặc chỉnh sửa thông tin cấu hình:***

Lợi dụng việc cấu hình thiếu an toàn như việc không xác thực thông tin trong việc gửi/nhận bản tin cập nhật (update) của router... mà kẻ tấn công sẽ thay đổi trực tiếp hoặc từ xa các thông tin quan trọng này, khiến cho những người dùng hợp pháp không thể sử dụng dịch vụ.

Ví dụ: hacker có thể xâm nhập vào DNS để thay đổi thông tin, dẫn đến quá trình biên dịch tên miền (domain) sang địa chỉ IP của DNS bị sai lệch. Hậu quả là các yêu cầu của máy trạm (Client) sẽ tới một tên miền khác (đã bị thay đổi) thay vì tên miền mong muốn.

- Phá hoại hoặc chỉnh sửa phần cứng:

Lợi dụng quyền hạn của chính bản thân kẻ tấn công đối với các thiết bị trong hệ thống mạng để tiếp cận phá hoại các thiết bị phần cứng như router, switch…

- **Cách phòng chống:**

Hậu quả mà DoS gây ra không chỉ tiêu tốn nhiều tiền bạc, và công sức mà còn mất rất nhiều thời gian để khắc phục. Vì vậy, hãy sử dụng các biện pháp sau để phòng chống DoS:

- Mô hình hệ thống cần phải được xây dựng hợp lý, tránh phụ thuộc lẫn nhau quá mức. Bởi khi một bộ phận gặp sự cố sẽ làm ảnh hưởng tới toàn bộ hệ thống.

- Thiết lập mật khẩu mạnh (strong password) để bảo vệ các thiết bị mạng và các nguồn tài nguyên quan trọng khác.

- Thiết lập các mức xác thực đối với người sử dụng cũng như các nguồn tin trên mạng. Đặc biệt, nên thiết lập chế độ xác thực khi cập nhật các thông tin định tuyến giữa các router.

- Xây dựng hệ thống lọc thông tin trên router, firewall… và hệ thống bảo vệ chống lại SYN flood.

- Chỉ kích hoạt các dịch vụ cần thiết, tạm thời vô hiệu hoá và dừng các dịch vụ chưa có yêu cầu hoặc không sử dụng.

- Xây dựng hệ thống định mức, giới hạn cho người sử dụng, nhằm mục đích ngăn ngừa trường hợp người sử dụng ác ý muốn lợi dụng các tài nguyên trên server để tấn công chính server hoặc mạng và server khác.

- Liên tục cập nhật, nghiên cứu, kiểm tra để phát hiện các lỗ hổng bảo mật và có biện pháp khắc phục kịp thời.

- Sử dụng các biện pháp kiểm tra hoạt động của hệ thống một cách liên tục để phát hiện ngay những hành động bất bình thường.

- Xây dựng và triển khai hệ thống dự phòng.

2.4.3 MAC Flooding:

Cách tấn công này cũng dùng kỹ thuật ARP Poisoning mà đối tượng nhắm đến là Switch. Hacker sẽ gửi những gói ARP Reply giả tạo với số lượng khổng lồ nhằm làm Switch xử lý không kịp và trở nên quá tải. Khi đó, Switch sẽ không đủ

sức thể hiện bản chất Layer2 của mình nữa mà broadcast gói tin ra toàn bộ các port của mình. Hacker dễ dàng bắt được toàn bộ thông tin trong mạng .

- **Chức năng chuyển mạch của Switch:**

Việc đưa thiết bị chuyển mạch vào một LAN có nhiều mục đích nhưng mục đích quan trong nhất là để chia một LAN ra thành nhiều vùng khác nhau nhằm giảm thiểu việc xung đột gói tin khi có quá nhiều thiết bị được nối vào cùng một môi trường truyền dẫn. Các vùng được phân chia này được gọi là các collision domain.Chức năng chính của switch là vận chuyển các frame lớp 2 qua lại giữa các collision domain này. Các collision domain này còn được gọi là các đoạn LAN (LAN segment).

Để có thể vận chuyển chính xác được gói tin đến đích, switch cần phải có một sơ đồ ánh xạ giữa địa chỉ MAC của các thiết bị vật lí gắn tương ứng với cổng nào của nó. Sơ đồ này được lưu lại trong switch và được gọi là bảng CAM (Content Address Memory).

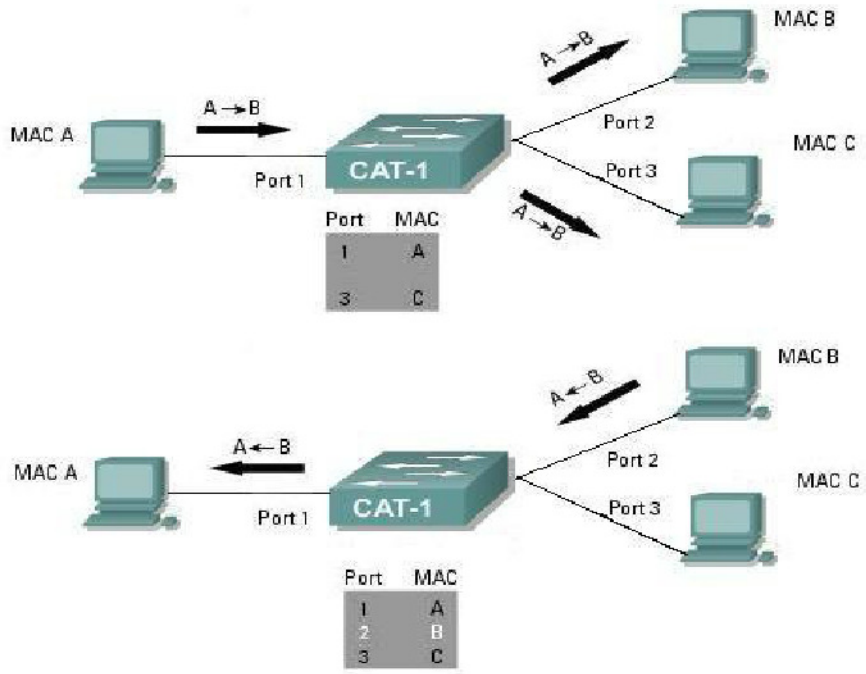
Quá trình vận chuyển gói tin qua switch có thể được mô tả như sau:

- Nếu địa chỉ MAC nguồn của gói tin chưa có trong bảng CAM; switch sẽ cập nhật với cổng tương ứng. Nếu địa chỉ MAC nguồn đã tồn tại trong bảng nhưng với một cổng khác, switch sẽ báo lỗi "MAC flapping" và huỷ gói tin.

- Nếu địa chỉ đích của gói tin là địa chỉ multicast hoặc địa chỉ broadcast hoặc là địa chỉ unicast nhưng ánh xạ của địa chỉ này không tồn tại trong bảng CAM trước đó thì gói tin sẽ được gửi ra tất cả các cổng của switch trừ cổng mà nó nhận được gói tin.

- Nếu địa chỉ đích của gói tin là địa chỉ unicast và ánh xạ của địa chỉ tồn tại trong bảng CAM đồng thời cổng mà nó nhận được gói tin khác với cổng mà gói tin cần được chuyển đi thì nó sẽ gửi gói tin đến chính xác cổng có trong bảng CAM.

- Các trường hợp còn lại, gói tin sẽ bị huỷ.



Hình 2.9 – Chức năng chuyển mạch của Switch.

Trong ví dụ trên, khi host A gửi bản tin đến host B. Do switch chưa có địa chỉ MAC của B trong bảng CAM của mình nên switch sẽ gửi broadcast ra mọi cổng còn lại đồng thời sẽ lưu lại địa chỉ MAC của A vào bảng CAM. Sau khi host B nhận được bản tin từ A; B gửi lại tin cho A. Khi đó, switch đã có địa chỉ của A nên sẽ gửi unicast tới port 1 đồng thời cập nhật địa chỉ MAC của B vào bảng CAM.

Các thao tác đối với bảng CAM của một switch [1]:

Để xem nội dung bảng CAM của switch, dùng lệnh:

Switch# show mac address-table dynamic [address mac-address |

interface type mod/num |vlan vlan-id]

Lệnh này sẽ liệt kê tất cả các địa chỉ MAC mà switch học được. Nếu muốn cụ thể hơn, có thể tìm được vị trí của host đã gắn vào switch bằng cách chỉ ra địa chỉ của nó hoặc có thể tìm được những địa chỉ MAC đã được học từ một giao diện nào đó.

Xem kích thước bảng CAM của switch, dùng lệnh:

Switch# show mac address-table count

Xoá các ánh xạ trong bảng CAM, dùng lệnh:

Switch# clear adress-table dynamic [address mac-address |

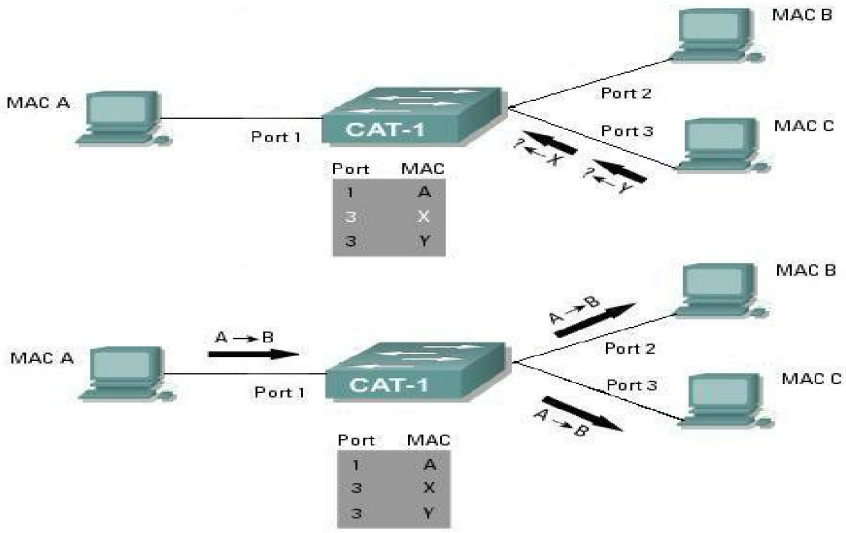
interface type mod/num |vlan vlan-id]

- **Tấn công làm tràn bảng CAM:**

- ***Nguyên lý tấn công:***

Kiểu tấn công làm tràn bảng CAM dựa vào điểm yếu của thiết bị chuyển mạch: bảng CAM chỉ chứa được một số hữu hạn các ánh xạ (ví dụ như switch Catalysh 6000 có thể chứa được tối đa 128000 ánh xạ) và các ánh xạ này không phải tồn tại mãi mãi trong bảng CAM [4]. Sau một khoảng thời gian nào đó, thường là 300 s; nếu địa chỉ này không được dùng trong việc trao đổi thông tin thì nó sẽ bị gỡ bỏ khỏi bảng.Khi bảng CAM được điền đầy, tất cả thông tin đến sẽ được gửi đến tất cả các cổng của nó trừ cổng nó nhận được. Lúc này chức năng của switch không khác gì chức năng của một hub.

Trong hình dưới, host C của kẻ tấn công gửi đi liên tục hàng loạt các bản tin có địa chỉ MAC nguồn là địa chỉ giả mạo (host X và host Y). Switch sẽ cập nhật địa chỉ của các host giả mạo này vào bảng CAM. Kết quả là khi host A gửi tin đến cho host B; địa chỉ của B không tồn tại trong bảng nên gói tin được switch gửi ra các cổng của nó và bản tin A chỉ gửi riêng cho B cũng sẽ được chuyển đến C.



Hình 2.10 – Mô hình tấn công làm ngập bảng CAM.

- ***Cách phòng chống:***

Nguyên lí chung của các phương pháp phòng chống là không để các gói tin có địa chỉ MAC lạ đi qua switch. Phương pháp phòng chống hiệu quả nhất là cấu hình port security trên switch 1. Đây là một đặc trưng cấu hình cho phép điều khiển việc truy cập vào cổng switch thông qua địa chỉ MAC của thiết bị gắn vào.

Khi switch nhận được một gói tin chuyển đến, nó sẽ kiểm tra địa chỉ MAC nguồn của gói tin với danh sách các địa chỉ đã được cấu hình trước đó. Nếu hai địa chỉ này khác nhau thì tuỳ theo sự cấu hình của người quản trị mà switch sẽ xử lí gói tin đến với các mức độ khác nhau.

Các lệnh cấu hình port security:

∗Switch(config-if)# switchport mode access

∗Switch(config-if)# switchport port-security: cho phép cổng được hoạt động trong chế độ port-security.

∗Switch(config-if)# switchport port-security maximum value (tuỳ chọn): câu lệnh cho phép cấu hình số địa chỉ MAC tối đa mà cổng có thể học tự động và cho phép các thiết bị này truyền dữ liệu qua. Mặc định thì cổng chỉ cho phép một

địa chỉ MAC (một thiết bị) được gán vào và số địa chỉ có thể nằm trong khoảng từ 1 đến 1024.

∗Switch(config-if)# switchport port-security mac-address mac_address (tuỳ chọn) : bên cạnh cách cấu hình cho phép switch học tự động địa chỉ MAC; có thể gán tĩnh một số địa chỉ MAC có thể truy cập vào một port. Nếu số lượng địa chỉ gán tĩnh mà nhỏ hơn số địa chỉ MAC switch có thể học tự động thì số địa chỉ MAC còn lại sẽ được học tự động.

∗Switch(config-if)# switchport port-security violation {protect | restrict | shutdown} (tuỳ chọn) : Đây là các biện pháp mà người quản trị có thể tiến hành khi một gói tin đến không phù hợp với yêu cầu của port-security (khi có nhiều hơn số địa chỉ MAC tối đa được học hoặc khi gói tin đến có địa chỉ MAC khác so với các địa chỉ MAC đã được cấu hình tĩnh). Các biện pháp xử lí có thể là :

Shutdown: cổng sẽ bị ngừng hoạt động; không nhận và chuyển gói tin.

Restrict: cổng chỉ cho phép các gói tin có địa chỉ MAC hợp lệ đi qua; các gói tin vi phạm sẽ bị huỷ. Đồng thời số lượng các bản tin vi phạm sẽ được thống kê và báo cho người quản trị biết.

Protect: cũng giống như trong trường hợp restrict, tuy nhiên việc vi phạm sẽ không được ghi lại.

Phương pháp này tuy có yêu cầu công việc của người quản trị tăng lên đôi chút tuy nhiên nó là phương pháp rất hiệu quả để khoá các gói tin không rõ nguồn gốc có ý định tấn công vào switch.

CHƯƠNG III: HỆ THỐNG IDS

3.1. Tổng quan Hệ thống IDS

Do sự gia tăng những cuộc xâm nhập mạng, cùng với sự phát triển của mạng Internet ngày càng trở nên phổ biến, các tổ chức đang phải tăng cường các hệ thống giám sát an ninh cho mạng. Gần đây hệ thống dò tìm xâm nhập (IDS: Intrusion Detection System) đang có được sự quan tâm nhiều hơn của các tổ chức do tính ứng dụng và tính an toàn cao. Chúng ta sẽ xem xét một số khái niệm trong hệ thống IDS và cấu trúc của nó.

3.1.1. Khái niệm về hệ thống IDS

IDS là một hệ thống phòng thủ có nhiệm vụ dò tìm những hành động mang tính thù địch trên mạng. Mục đích chính của IDS là dò tìm và có thể thực hiện ngăn cản những hành động tấn công vào hệ thống an ninh hoặc những tấn công phá hoại bao gồm cả việc do thám và thu thập tài liệu. Đặc điểm chính của hệ thống dò tìm xâm nhập là khả năng cung cấp cách xác định hành động không mong đợi và tạo ra cảnh báo tới người quản trị mạng và có thể thực hiện ngăn chặn những kết nối không mong muốn.

Theo một định nghĩa trên trang web www.securitydocs.com, dò tìm xâm nhập là một quá trình xác định và đáp ứng lại những hành động tấn công nhằm vào hệ máy tính và tài nguyên mạng. Ngoài ra IDS còn có khả năng xác định nguồn gốc những cuộc tấn công. Thực tế có nhiều thiết bị an ninh sử dụng những công nghệ dùng trong IDS, tuy nhiên không phải mọi thiết bị dò tìm đều là hệ thống IDS:

- Hệ thống ghi nhật ký mạng thường dò tìm những tấn công DoS trên mạng.

Đây là những hệ thống theo dõi lưu lượng mạng.

- Những công cụ dùng để kiểm tra lỗi trong hệ điều hành và các chương trình ứng dụng mạng. Đây thường là những công cụ để kiểm tra mạng.
- Những chương trình chống virus được thiết kế để phát hiện và diệt các chương trình virus, trojan, worm… Những chương trình này có đặc điểm rất giống với hệ thống dò tìm xâm nhập và thường cung cấp cho hệ thống một công

cụ phát hiện vi phạm an ninh rất hiệu quả.

- Tường lửa (firewall), các hệ thống Proxy.
- Hệ thống bảo mật, mã hóa, ví dụ như VPN, SSL...

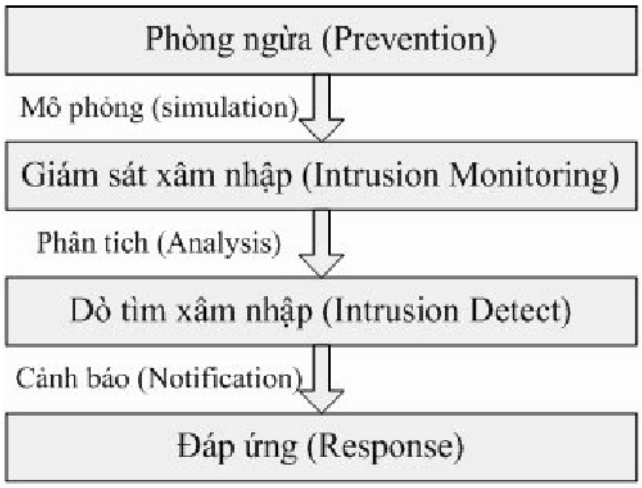
Nguyên tắc phân loại tấn công và xâm nhập

Hệ thống IDS dùng để chống lại những vi phạm về an ninh trong mạng, vì thế chúng ta cần hiểu rõ hơn về những hành động gây nguy hiểm cho mạng. Có thể định nghĩa một số hành động đó như sau:

- Xâm nhập: Một loạt những hành động liên quan với nhau nhằm đe dọa tính an toàn của nguồn tài nguyên mạng từ một truy nhập bất hợp pháp.
- Hành động xảy ra: Sự vi phạm chính sách an ninh mạng và được xác định như là một sự xâm nhập thành công.
- Tấn công: Những cố gắng để truy nhập vào một hệ thống nhưng chưa thành công.
- Mô hình xâm nhập: Mô hình các hành động theo thời gian tạo ra một sự xâm nhập. Kẻ xâm nhập bắt đầu tấn công với những hành động mở đầu và tiến tới truy nhập thành công. Trên thực tế, một tấn công từ bất kỳ một người nào, kể cả người quản trị, cũng bị xem là hành động đe dọa tới an ninh của mạng.

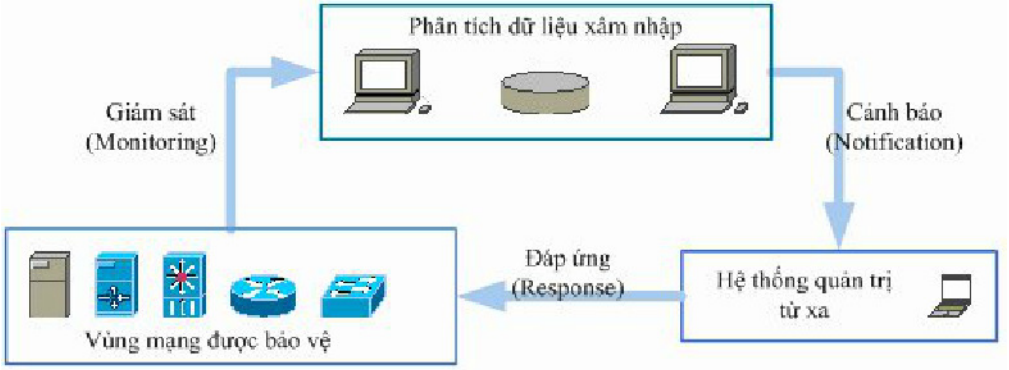
Hoạt động của hệ thống

Chức năng chính của hệ thống IDS là bảo vệ mạng và hệ thống máy tính bằng cách dò tìm những tấn công và có thể lặp lại chúng. Việc dò tìm những hoạt động tấn công phụ thuộc vào số lượng và kiểu tấn công. Ngăn chặn xâm nhập đòi hỏi một sự kết hợp tốt giữa dò tìm và giăng bẫy. Chuyển hướng chú ý của hành động tấn công cũng là một nhiệm vụ. Cả hai hệ thống IDS theo thời gian thực và hệ thống phân tích nhật ký đều cần được giám sát. Số liệu đưa ra từ hệ thống IDS cần được kiểm tra kỹ để không bỏ sót bất kỳ một dấu hiệu tấn công



Hình 3.1 – Các hoạt động của hệ thống IDS

Khi một hoạt động xâm nhập xảy ra, hệ thống IDS sẽ tạo ra một tín hiệu cảnh báo đối với người quản trị hệ thống, quản trị mạng. Bước tiếp theo có thể được xử lý bởi người quản trị hoặc từ hệ thống IDS, có thể là ngắt kết nối, kthúc phiên làm việc hoặc chỉ chuyển hướng hoạt động đó sang hệ thống khác, điều này phụ thuộc vào chính sách an ninh của từng mạng.



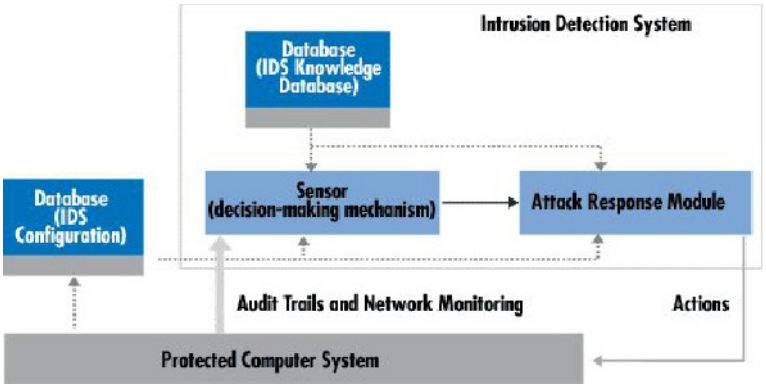
Hình 3.2 – Hạ tầng hệ thống IDS

Mặc dù nhiệm vụ của hệ thống IDS có thể thay đổi nhưng việc dò tìm những hoạt động tấn công vẫn là nhiệm vụ chính, chức năng chính của hệ thống. Sẽ rất tốt đối với an ninh mạng nếu chúng ta nghiên cứu về các cuộc tấn công và thực hiện biện pháp ngăn ngừa trước những tấn công đó trong tương lai.

Đôi khi hệ thống IDS cũng tạo ra những cảnh báo sai, đặc biệt khi gửi một miêu tả về một lỗi hay một loại virus nào đó thông qua mạng, qua dịch vụ thư điện tử..

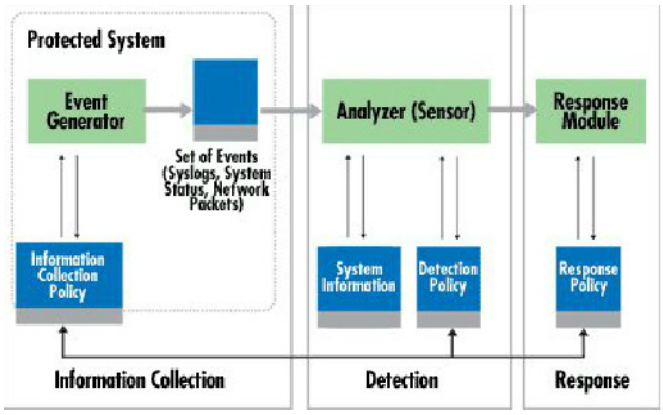
3.1.2. Cấu trúc hệ thống IDS

Bất kỳ một hệ thống IDS nào cũng có thành phần lõi là một bộ cảm biến (phân tích), có nhiệm vụ dò tìm những hành động xâm nhập mạng. Bộ cảm biến này có cơ chế để tạo ra những quyết định về một hành động có phải là hành động xâm nhập mạng hay không? Bộ phân tích này sẽ thu nhận tín hiệu gốc từ ba nguồn chính: Cơ sở dữ liệu trong hệ thống IDS, từ hệ thống syslog, từ nhật ký của mạng. Hệ thống syslog có thể chứa cả thông tin cấu hình, thông tin xác thực người dùng, v.v… Những thông tin này tạo cơ sở cho quá trình tạo ra luật hoạt động xác định hành động xâm nhập.



Hình 3.3 – Cấu trúc khối hệ thống IDS

Bộ cảm biến được tích hợp với các thành phần khác, như bộ phản hồi dữ liệu thu được, bộ tạo sự kiện (hình 2.4). Bộ thu nhận dữ liệu sử dụng chính sách của bộ tạo sự kiện, trong đó có định nghĩa các kiểu lọc thông tin cảnh báo. Bộ tạo sự kiện thường tạo ra những dữ liệu giống như hệ điều hành, lưu lượng mạng, ứng dụng, những dữ liệu này được xử lý và ghi lại bởi hệ thống ghi nhật ký. Tập các dữ liệu thông tin này được lưu giữ trong hay ngoài hệ thống được bảo vệ tùy thuộc vào chính sách an ninh của từng mạng. Trong một số trường hợp dữ liệu không được lưu giữ mà được truyền trực tiếp tới bộ phân tích (cảm biến), ví dụ như gói tin mạng.



Hình 3.4 – Các thành phần của IDS

Bộ phân tích có nhiệm vụ lọc những tín hiệu phù hợp từ tập các dữ liệu được chuyển tới để dò tìm những hoạt động khả nghi. Bộ phân tích sử dụng cơ sở dữ liệu những chính sách an ninh để dò tìm, bao gồm các dữ liệu về các hoành động tấn công, dữ liệu về hoạt động bình thường, các tham số cần thiết. Ngoài ra, cơ sở dữ liệu này còn chứa những tham số cấu hình của hệ thống IDS, bao gồm cả phương thức liên hệ với module phản hồi. Bộ cảm biến cũng có thể sử dụng dữ liệu riêng cho những hoạt động phức tạp hơn, ví dụ đa nhiệm...

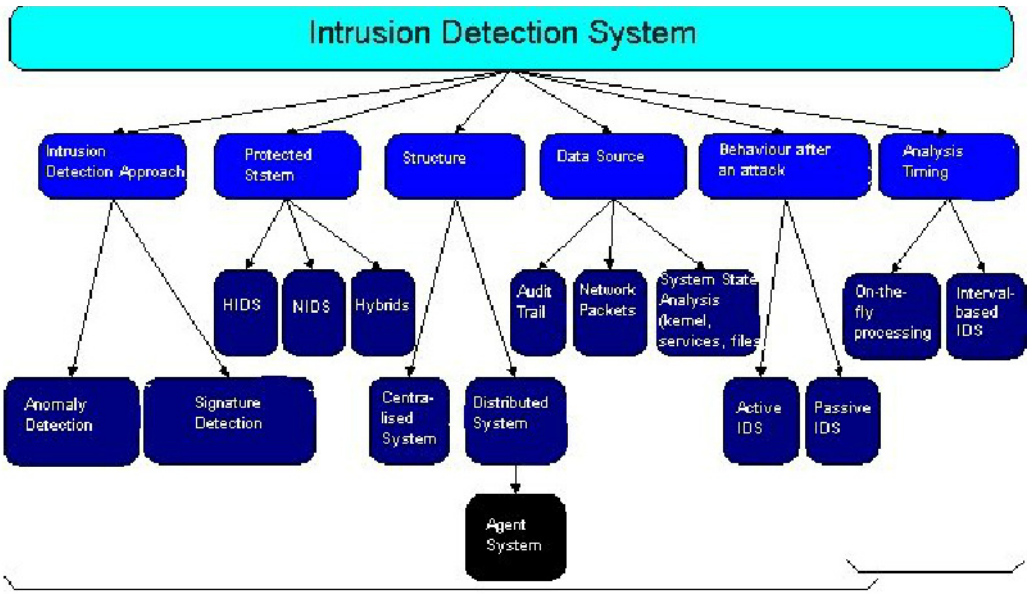
3.2. Phân loại IDS

Về cơ bản hệ thống IDS được quan tâm chủ yếu đến phương thức dò tìm hành động tấn công. Hệ thống này sử dụng hai phương thức chính là dò tìm theo mẫu và do tìm sự bất thường. Cả hai phương thức trên đều có những ưu điểm và nhược điểm riêng, chúng ta sẽ xem xét kỹ hơn ở mục 3.

Tuy nhiên nếu xét trong một mạng với đầy đủ các thành phần mạng, chúng ta cần phải quan tâm đến vùng dữ liệu, phương thức xử lý dữ liệu…, theo các tiêu chí đó, chúng ta có thể phân loại hệ thống IDS như sau:

- Theo phương thức dò tìm: Dò tìm bất thường, dò tìm theo mẫu.
- Theo vùng dữ liệu: Hệ thống trạm, hệ thống mạng, hệ thống pha trộn.
- Theo cấu trúc hệ thống: Hệ thống tập trung, hệ thống phân tán.
- Theo nguồn dữ liệu được xử lý: Dữ liệu nhật ký, gói tin mạng, trạng thái hệ thống.

- Theo phương thức xử lý theo thời gian: Xử lý theo thời gian thực, xử lý theo chu kỳ.
- Theo các hành động đáp ứng: Hệ thống hoạt động chủ động, hệ thống hoạt động



.

Hình 3.5 – Phân loại Hệ thống IDS

Trên thực tế việc phân chia này không có biên giới rõ ràng, vì nhiều hệ thống có thể tích hợp nhiều công nghệ khác nhau sao cho có thể đạt được hiệu quả cao nhất. Vì thế chỉ có 3 kiểu phân loại chính là theo vùng dữ liệu, theo phương thức xử lý dữ liệu theo thời gian và theo phương thức dò tìm.

3.2.1. Phân loại theo vùng dữ liệu

Khi quan tâm đến vùng dữ liệu cần được kiểm tra để phát hiện xâm nhập, chúng ta có thể chia hệ thống IDS thành hệ thống trạm nếu dùng để phân tích dữ liệu cho một máy chủ hoặc hệ thống mạng nếu dùng để phân tích dữ liệu cho toàn mạng.

Hệ thống trạm (Host based system)

Dùng cho việc dò tìm những hành động xâm nhập vào một máy chủ hoặc một hệ thống đơn lẻ, bao gồm các chức năng:

- Dò tìm, theo dõi kết nối vào ra: Hệ thống này dùng để kiểm tra các kết nối mạng từ ngoài vào hoặc từ trong hệ thống ra mạng ngoài, thường được dùng để ngăn ngừa các kết nối hoặc cảnh báo các hành động dò tìm mạng.
- Kiểm tra lưu lượng mạng vào ra của máy chủ: Hệ thống này thường dùng dò tìm những dữ liệu có tính nhạy cảm hoặc cảnh báo sự quá tải.
- Theo dõi những hành động vào ra: Hệ thống này dùng theo dõi quá trình truy nhập hoặc thoát khỏi một máy chủ cần được theo dõi hoặc một hệ thống.
- Theo dõi hành động của quản trị: Dùng theo dõi những hành động bất thường của tài khoản có quyền cao nhất trên hệ thống, cảnh báo và phòng chống trường hợp giả mạo hoặc bị chiếm quyền hệ thống.
- Theo dõi sự thay đổi của hệ thống: Dùng để theo dõi những sự thay đổi đối với những file có tính quan trọng trên hệ thống (ví dụ file cấu hình hệ thống).

Hệ thống trạm được thiết lập để cung cấp khả năng bảo vệ cho một máy chủ đặc biệt nào đó. Thông thường nó không chỉ có module giám sát mà còn cung cấp cả các module có tính năng phản ứng lại các hành động tấn công. Một số sản phẩm có thể kể tới hiện nay như Snort, Dragon Squire, Emerald eXpert-BSM, NFR HID.

Hệ thống mạng (Network based system)

Thực hiện quá trình tổng hợp và phân tích toàn bộ lưu lượng vào ra trên tất cả các cổng, các giao diện của mạng. Nó không chỉ xử lý dữ liệu đến một máy đặc biệt nào đó mà có thể phân tích lưu lương cho cả một phân đoạn mạng. Thông thường hệ thống NIDS được thiết lập trên một thành phần hoạt động ở chế độ thụ động (passive) nhờ đó nó có thể thu nhận mọi tín hiệu mà không bị phát hiện ra trên mạng. Trong một số trường hợp NIDS cũng có thể được thiết lập trên những thiết bị mạng đang hoạt động, ví dụ như bộ định tuyến (router).

Hoạt động dò tìm xâm nhập là công việc thuần túy thống kê dữ liệu, nên một hệ thống NIDS có thể được phân chia thành các module độc lập theo các chức năng như các chức năng theo dõi lưu lượng, chức năng thu nhận các gói tin trên

một đoạn mạng mà không cần phân tích, chức năng phân tích những dữ liệu thu nhận được… Một số sản phẩm có thể kể đến hiện nay là: Cisco Secure IDS (NetRanger), Hogwash, Dragon, E-Trust IDS.

Hệ thống pha trộn

Nếu chúng ta quan tâm đến sự pha trộn giữa HIDS và NIDS sẽ tạo ra một kiểu hệ thống IDS là NNIDS (Network Node IDS). Trong hệ thống này nhiều agent được thiết lập trên các máy chủ (server, node) trong mạng cần được bảo vệ, thực tế NNIDS hoạt động giống như là NIDS cho từng máy chủ, các agent này sẽ thu nhận dữ liệu trực tiếp trên các máy chủ đó. Việc xử lý dữ liệu có thể được thực hiện ngay trên agent hoặc được đưa về bộ xử lý trung tâm để xử lý. NNIDS thường được sử dụng trong những mạng mang tính bảo mật cao, ví dụ như các ứng dụng thương mại điện tử, những gói tin thường được mã hóa và chỉ có chính máy chủ đó mới có thể giải mã được. Tuy nhiên hệ thống NNIDS chỉ là sự lai tạp giữa hệ thống trạm và mạng, vì thế chúng ta chỉ cần quan tâm chủ yếu đến hai hệ thống là HIDS và NIDS.

3.2.2. Phân loại theo phương thức xử lý dữ liệu

Hệ thống dò tìm xâm nhập có thể chạy ở chế độ thời gian thực hoặc theo chu kỳ, và vì thế chúng có phương thức xử lý dữ liệu là khác nhau.

Xử lý dữ liệu nhật ký (Audit trail proccessing)

Có rất nhiều kết quả liên quan đến quá trình xử lý nhật ký sự kiện hệ thống, vì thế sẽ rất rủi ro nếu lưu giữ nhật ký bằng một file trên hệ thống. Tốt hơn là người quản trị nên lưu giữ một bản nhật ký thông qua hệ thống lưu trữ mạng. Ngoài ra với chức năng lưu nhật ký sự kiện, hệ thống sẽ tốn một lượng tài nguyên nhất định để thực hiện. Một số ứng dụng nên thực hiện nén dữ liệu trước khi gửi để giảm lưu lượng mạng, một số ứng dụng khác không nên thực hiện nén để tránh làm ảnh hưởng đến tải của hệ thống.

Có nhiều kết quả liên quan đến tiến trình xử lý nhật ký hệ thống. Việc lưu giữ bản ghi các sự kiện lên một file đơn cần phải tránh bởi vì những kẻ xâm nhập có thể lợi dụng đặc điểm này làm thay đổi nhật ký hệ thống. Tốt nhất là

nên lưu giữ một bản trên hệ thống lưu giữ trên mạng, điều này có thể sẽ gây một ảnh hưởng nào đó đến năng lực hoạt động của mạng và hệ thống.

Ngoài ra nếu nhìn theo quan điểm chức năng, việc ghi lại mọi sự kiện của hệ thống có thể sẽ ảnh hưởng tới tài nguyên của hệ thống, nén file có thể làm giảm tải các gói tin trên mạng . Thực tế việc xác định những thông tin nào cần ghi lại trong nhật ký sự kiện hệ thống là khá khó khăn bởi vì nếu ghi thiếu, chắc chắn sẽ có một kiểu tấn công chưa biết bị bỏ qua. Cũng rất khó để có thể xác định chính xác kích thước của hệ thống file ghi sự kiện hệ thống, thường phải thông qua kinh nghiệm để ước lượng. Nhìn chung điều này phụ thuộc lớn vào giải pháp của hệ thống IDS, nhưng một điều chắc chắn là hệ thống lưu giữ nhật ký phải lưu được những thông tin để phục vụ cho việc phân tích sau đó. Dưới đây là một số lý do đối với việc cần thiết phải có hệ thống IDS sử dụng công cụ phân tích nhật ký:

- Dò tìm những tấn công thông qua phân tích dữ kiện đã xảy ra.
- Dò tìm những hành động xâm nhập có chu kỳ.
- Xác định chính xác kẻ xâm nhập.
- Xác định điểm yếu của hệ thống

Sự phát triển của việc truy nhập, đặc điểm người dùng, đặc điểm lưu lượng mạng là rất quan trọng đối với hệ thống IDS dựa trên phương thức dò tìm sự bất thường.

Bản ghi kiểm tra có thể cung cấp phương thức chống lại sự tấn công mạng. Nguyên lý của hệ thống IDS dựa trên thông tin ghi lại sự kiện mạng cần phải có những khả năng sau:

- Cho phép thay đổi tham số để dễ dàng ghi lại những hoạt động của hệ thống theo những cách khác nhau.
- Cung cấp khả năng loại bỏ việc ghi nhật ký để tránh trường hợp mạng, hệ thống bị tấn công DoS.
- Đối với việc xử lý file lớn, việc xử lý sẽ sử dụng các kỹ thuật khác, ví dụ tối ưu hóa dữ liệu, trí tuệ nhân tạo….
- Tối thiểu hóa hợp lý việc sử dụng tài nguyên mạng cho mục đích ghi nhật

ký.

Xử lý thời gian thực (on-the-fly proccessing)

Với phương thức xử lý thời gian thực, hệ thống IDS hoạt động đáp ứng lập tức đối với sự kiện của mạng. Nhìn chung, một luồng gói tin là được kiểm tra liên tục, với phương thức này, hệ thống IDS sử dụng kiến thức có sẵn về hoạt động mạng tại thời điểm theo dõi để phát hiện những tấn công tại thời điểm đó, không tìm kiếm những tấn công đã qua.

Sự phức tạp của việc tính toán và thuật toán ở đây đã hạn chế tính nhanh và hiệu quả của quá trình, mà thường là rất đơn giản. Hạn chế này là do sự kết hợp giữa hai yếu tố chính: khả năng dò tìm tấn công và cơ chế xử lý dữ liệu.
Tại một thời điểm, những công cụ xử lý yêu cầu một lượng lớn bộ đệm, vì không có dữ liệu cần lưu trữ. Vì thế, một hệ thống IDS có thể thỉnh thoảng bị mất gói tin, do độ tin cậy của việc xử lý nhiều gói tin là không cao.

Hệ thống IDS thời gian thực có những ưu điểm sau:

- Hệ thống này có ưu thế hơn trong quá trình đang điễn ra tấn công mạng và thậm chí khi đã ngăn chặn được tấn công.
- Khả năng bao phủ rộng các lỗ hổng an ninh của mạng với nhiều dạng tấn công khác nhau, thậm chí cả DoS.
- Tài nguyên hệ thống ít lãng phí hơn so với hệ thống xử lý thông tin nhật ký.

Nhược điểm của hệ thống:

- Việc xác định nguồn tấn công là dựa trên địa chỉ mạng được lấy ra từ gói tin. Việc này sẽ gặp khó khăn khi bị giả mạo địa chỉ, những tấn công giả mạo địa chỉ sẽ khó truy tìm và ngăn chặn hơn.
- Không thể cung cấp cho mạng nếu trong đó có thực hiện mã hóa gói tin.
- Bộ phân tích chỉ sử dụng một phần của gói tin nên khả năng dò tìm cũng bị hạn chế.
- Việc thực hiện quét mạng liên tục làm giảm đi thông lượng của phân mạng có chứa hệ thống IDS. Điều này đặc biệt nghiêm trọng khi IDS sử dụng gần với thiết bị tường lửa (Firewall).

3.2.3. Phân loại theo phương pháp dò tìm xâm nhập

Một hệ thống IDS có khả năng phân biệt được hoạt đông thông thường và bất thường của người dùng. Tuy nhiên để phiên dịch những hoạt động của người dùng ra thành một quyết định chính xác của máy tính thường không đơn giản chút nào. Các hoạt động này thường không có một ranh giới rõ rệt. Để có thể phân loại được các hoạt động, hệ thống IDS cần áp dụng những phương pháp dò tìm đạt hiệu quả cao. Hiện nay có hai phương pháp thường áp dụng là dò tìm bất thường (anomaly detect) và dò tìm theo mẫu (signature detect).

Dò tìm bất thường (anomaly detect)

Các mẫu hoạt động thường được phân chia thành hai loại là của người dùng và của hệ thống. Trong các hệ thống IDS hoạt động theo cơ chế dò tìm bất thường, một bộ dò tìm sẽ tạo nên một cấu hình có thể mô tả được hoạt động thường sử dụng và sử dụng dữ liệu đó để có thể nhận ra được sự khác biệt giữa hoạt động bình thường và khi có tấn công.

Để tạo được một cấu hình cho các hoạt động của người dùng, một yêu cầu là phải khởi tạo một cấu hình chuẩn ban đầu, sau đó hệ thống có thể tự học để nhận biết được những hoạt động hợp lệ trên hệ thống. Ở đây xảy ra một vấn đề là đối với nhưng hệ thống tự học, những kẻ xâm nhập giỏi có thể lợi dụng để dẫn hệ thống đến việc học các hoạt động xâm nhập như các hoạt động thường. Một cấu hình không thích hợp sẽ dẫn đến không phát hiện được đầy đủ các cuộc xâm nhập. Ngoài ra việc cập nhật liên tục cấu hình đó cũng gặp nhiều khó khăn và mất nhiều thời gian.

Với một cấu hình định trước, tất cả những hoạt động không được tìm thấy trong cấu hình đó đều được coi là những hành động có nghi vấn. Vì thế đặc điểm của hệ thống như vậy là có mức độ an ninh rất cao, tuy nhiên xu hướng tạo ra những cảnh báo sai là cũng khá phổ biến.

Lợi ích của nguyên lý dò tìm bất thường là có thể phát hiện những tấn công mới, những hoạt động bất thường có thể được phat hiện mà không cần biết trước những đặc điểm của hoạt động đó. Hệ thống IDS sử dụng nguyên lý dò tìm bất thường hoạt động không phụ thuộc nhiều vào hệ điều hành, có thể dò tìm

được những hoạt động lạm dụng quyền của người dùng quản trị hoặc thông thường.

Nhược điểm lớn nhất của nguyên lý dò tìm sự bất thường:

- Tỉ lệ thông báo sai khá lớn, hệ thống không hoạt động trong quá trình cập nhật lại cấu hình và học lại. Vì thế những hoạt động xâm nhập trong khi đó đều không được theo dõi.
- Hoạt động của người dùng thay đổi theo thời gian, không bất biến, vì thế yêu cầu đặt ra đối với hệ thống là thường xuyên phải cập nhật dữ liệu.
- Hệ thống sẽ bị suy giảm khả năng miễn dịch trong quá trình học lại những dữ liệu về hoạt động của người dùng.

Dò tìm theo mẫu (signature detect)

Hệ thống dò tìm theo dấu hiệu thực hiện so sánh các hành động thu nhận được với những hành động tấn công đã biết trước, được gọi là các mẫu tấn công (attack signature). Các dấu hiệu về hành động sai, hành động tấn công thường được chia thành hai loại sau:

- Mẫu tấn công (attack signature): Miêu tả các hành động có thể gây tác động xấu tới an ninh mạng. Thông thường những hành động này được biểu diễn bởi một mối quan hệ theo thời gian giữa một loạt các hành động liên quan.
- Chuỗi văn bản (text strings): Các mẫu phù hợp với một chuỗi văn bản được dùng để tìm kiếm những hành động khả nghi trên mạng.

Bất kỳ một hành động nào không được coi là cấm một cách rõ ràng thì đều được hệ thống cho phép qua. Vì thế tính chính xác của phương pháp này là rất cao. Thông thường hệ thống sử dụng dò tìm theo mẫu không đạt được sự hoàn thiện và không miễn dịch được với các tấn công mới.

Hiện nay có hai hướng nghiên cứu chính sử dụng trong hệ thống dò tìm theo mẫu:

- Kiểm tra các gói tin lớp IP và TCP: Có rất nhiều các cuộc tấn công nhằm khai thác lỗ hổng trong gói tin IP, ICMP, TCP, UDP. Chỉ với một thủ tục kiểm tra đơn giản bằng việc thiết lập các cờ tại các gói tin đặc biệt, nó có thể xác định được gói tin đó có hợp lệ hay không. Tuy nhiên khó khăn xảy ra khi các gói

tin bị phân mảnh và cần ghép lại. Điều này thường được những kẻ tấn công khai thác để vượt qua các hệ thống IDS.

- Kiểm tra giao thức lớp ứng dụng: Có rất nhiều tấn công nhằm khai thác lỗ hổng của các chương trình ứng dụng có sử dụng các giao thức tầng ứng dụng. Để dò tìm dược những tấn công kiểu này có hiệu quả, hệ thống IDS cần thực hiện được rất nhiều các giao thức.

Phương thức dò tìm theo mẫu có nhiều ưu diểm như: ít cảnh báo sai, thuật toán đơn giản, dễ tạo dữ liệu, dễ thực thi và sử dụng ít tài nguyên. Tuy nhiên hệ thống IDS sử dụng phương thức dò tìm này có rất nhiều nhược điểm:

- Việc cập nhật thông tin dữ liệu là khó khăn.

- Không thực hiện dò tìm được những tấn công mới, tấn công chưa biết. Một yêu cầu đặt ra là mẫu về những cuọc tấn công phải luôn luôn được cập nhật.
- Những mẫu về tấn công hầu hết đều phụ thuộc vào môi trường hoạt động, vì thế những sản phẩm thường phai đi kèm theo cả hệ điều hành, ứng dụng….
- Gặp khó khăn khi cần phát hiện những tấn công từ bên trong.

3.3. Phương pháp dò tìm sự xâm nhập dựa theo dấu hiệu khác thường của hành động (Anomaly-based Intrusion Detection)

3.3.1 Dò tìm sự khác thường

Hacker là những người có hiểu biết rất rõ về việc khai thác những lỗ hổng của hệ thống. Rất nhiều công cụ tấn công trở nên phổ biến và được gọi là những tấn công nổi tiếng. Với những tấn công này, hệ thống IDS sử dụng dữ liệu có sẵn để so sánh (dò tìm theo mẫu), nhưng với những hacker thông minh họ sẽ thực hiện thay đổi một chút dấu hiệu đó để đánh lừa hệ thống. Vì thế dò tìm theo mẫu trở nên lạc hậu và không phát hiện được hết những cuộc tấn công.

Dò tìm xâm nhập dựa trên những dấu hiệu khác thường là một phương thức giúp hệ thống có thể phát hiện được những tấn công mới. tuy nhiên để có được hiệu quả cần dùng kết hợp giữa dò tìm sự khác thường với dò tìm theo dấu hiệu.

Dò tìm sự khác thường đưa ra những tín hiệu cảnh báo trên hệ thống ngay khi phát hiện một haọt động có dấu hiệu khác biệt xảy ra trên mạng. Tất cả các sự kiện, nội dung, hoạt động đều được quan tâm tới và mọi sự sai lệnh so với hoạt động bình thường được định nghĩa trước đều được đánh dấu và ghi lại. Những hoạt động bình thường có thể được lập trình, thống kê để ghi lại dựa trên quá trình học hoặc các mô hình toán học.

Một số ví dụ về hoạt động khác thường:

- Lưu lượng http trên cổng TCP=53, sai lệch về cổng dịch vụ
- Các dịch vụ cửa hậu (backdoor) nhưng sử dụng các cổng dịch vụ khác, ví dụ các dịch vụ chia sẻ tập tin dùng cổng TCP=80
- Một đoạn mã nhị phân trong trường mật khẩu
- Quá nhiều gói tin UDP so với gói tin TCP, sai lệnh thống **kê.**
- Lưu lượng http vào máy chủ nhiều hơn là vào máy trạm, khác thường về hoạt động của dịch vụ

3.3.2 Sự khác biệt của hai phương pháp

Khi giám sát an ninh một mạng, hệ thống IDS có thể sử dụng kỹ thuật dò tìm theo dấu hiệu hay dò tìm sự khác thường. Có những ưu nhược điểm riêng cho từng phương pháp, việc sử dụng cả hai phương thức là tốt nhất cho mạng. Thông thường dấu hiệu có liên quan tới một tập những điều kiện mô tả trực tiếp hoạt động xâm nhập theo mào đầu của gói tin hay nội dung tải. Lịch sử cho thấy phương pháp dò tìm dấu hiệu là phổ biến hơn. Phương pháp này dựa vào dữ liệu dấu hiệu tấn công và khi một hay nhiều dữ liệu phù hợp với mẫu quan sát, tín hiệu cảnh báo được phát ra và sự kiện đó được lưu lại. Dò tìm xâm nhập dựa vào dấu hiệu chỉ thực sự hiệu quả khi có dữ liệu tốt. Nếu dữ liệu không đầy đủ sẽ không bắt được hết các cuộc tấn công. Ngoài ra nếu chúng ta quan tâm tới việc hacker dành nhiều thời gian cho để thiết kế những tấn công đánh lừa hệ

thống thì hệ thống dò tìm dựa vào dấu hiệu thực sự không đạt được hiệu quả cao.

Dò tìm dựa vào sự khác thường thì lại khác, tạo ra một nghiên cứu chung khi tìm kiếm sự đe dọa tới mạng. Một giới hạn về hành động được coi là bất thường sẽ được phát triển và khi bất kỳ một hành động nào nằm ngoài khoảng giới hạn đó đề bị đánh dấu và ghi lại. Giống dò tìm theo dấu hiệu, dò tìm sự khác thường cũng dựa trên dữ liệu thông tin cho biết một hành động là bình thường hay bất thường, nó được gọi là profile. Đây là điểm quan trọng nhất đối với tính hiệu quả của hệ thống.

Tất cả dữ liệu trong hồ sơ (Profile)

Để một hệ thống dò tìm xâm nhập dựa vào tính dị thường hoạt động hiệu quả cần có một profile lớn, có thể miêu tả được tất cả những hành động thông thường của mục tiêu (có thể là một máy chủ hoặc một phân mạng). Một profile chứa danh sách tổng hợp các biến và giá trị đặc tả mục tiêu cần quan sát. Một profile lớn phải ổn định và tin cậy, khi lấy thông tin về mục tiêu. Một profile hiệu quả phải thích ứng được với những sự kiện an ninh xảy ra. Để tạo được một profile hiệu quả cần có sự thu thập thông tin. Ví dụ một profile có thể chứa các kiểu thông tin sau:

- Mẫu miêu tả các câu lệnh xuất hiện trong phiên làm việc, ví dụ một phiên làm việc bao giờ cũng chứa các lệnh xác thực (authentication)
- Sắp xếp kiểu nội dung với các trường khác nhau của giao thức, ví dụ trường mật khẩu phải có độ dài từ 8 đến 64 ký tự trong bảng mã ASCII
- Mẫu kết nối giữa máy chủ được bảo vệ và mạng ngoài, ví dụ với máy chủ Oracle, kết nối được thực hiện từ 3 máy trạm Oracle định trước.
- Tỉ lệ và sự bùng nổ lưu lượng mạng, ví dụ ở một phân đoạn mạng trong không thể có các gói tin IP phân đoạn liên tục trong một phút với hơn 100 gói tin trên một giây.

Ngoài ra các profile cần có khả năng tự học, đặc biệt là những profile về lưu lượng mạng. Một profile thích nghi có thể tính được sự thay đổi thông thường để tránh cảnh báo sai. Cơ chế tự học đảm bảo khả năng phát triển rộng và thành công. Đầu tiên rất khó phân tích và thiết lập các profile một cách nhân công, vì việc thống kê sự thay đổi là rất phức tạp. Tiếp theo với hy vọng lớn cung cấp khả năng dò tìm tại nhiều mức lưu lượng để đạt được sự bảo vệ nhiều tầng, tuy nhiên việc thống kê tại tất cả các mức là không cố định trong hầu hết các tổ chức. Với việc tự học, cơ chế dò tìm dựa vào sự khác thường có thể học được những thay đổi thông thường của luồng lưu lượng và từ đó xây dựng được những profile có hiệu quả cao.

Bởi vì phương pháp này cung cấp khả năng tìm kiếm những hành động được coi là mới và khác thường, nên nó rất hiệu quả trong việc cảnh báo sớm nguy cơ bị tấn công. Những cảnh báo này bao gồm cả những hành động tấn công do thám, hoạt động cửa hậu (backdoor) và những lỗi bảo mật mạng. Ngoài ra nó cũng hữu ích trong việc tìm những tấn công như sau:

- Tấn công tràn bộ đệm mới
- Những tấn công khai thác lỗ hổng mới
- Những tấn công không biết trước
- Biến thể của các cuộc tấn công trong môi trường mới

Cũng cần lưu ý rằng dò tìm tấn công dựa vào sự khác thường cung cấp khả năng phòng ngừa tốt nhất cho mạng chỉ khi kết hợp với dò tìm dựa theo dấu hiệu. Với những tấn công đã biết, nó cung cấp khả năng tìm kiếm chính xác với thời gian ngắn nhất. Trong cách kết hợp này, những tấn công đã biết, chưa biết hay những tấn công mới đều bị chặn.

3.3.3 Những trở ngại, khó khăn

Không phải mọi sự bất thường đều là hành động nhằm xâm nhập hệ thống. Với hệ thống IDS sử dụng phương pháp dò tìm xâm nhập dựa vào sự khác thường có những nhược điểm sau:

- Hay tạo ra những cảnh báo sai do những thay đổi về mạng và các ứng dụng
- Do sự tổng hợp và trích dẫn được sử dụng trong việc tạo ra các profile, những cảnh báo được phát ra có thể chứa không đầy đủ các thông tin cho những phân tích liên quan
- Việc xác định một hành động khác thường có phải là xâm nhập hệ thống hay không có thể là một quá trình tốn thời gian. Ví dụ một kiểu khai thác lỗi sử dụng một câu lệnh lỗi trong phiên làm việc có thể chỉ được phát hiện khi phiên làm việc đã kết thúc, điều này là quá muộn đối với hệ thống. Mỗi một công nghệ đều có những điểm yếu, những điểm yếu này có thể tồn tại trong hệ điều hành, giao thức hay thiết bị mạng.

3.4. Xử lý dữ liệu.

Tùy thuộc vào từng mô hình, cơ chế xử lý dữ liệu của hệ thống dò tìm xâm nhập có sự khác nhau về công nghệ, phương thức. Dưới đây là một số công nghệ thường được sử dụng:

Hệ chuyên gia: Những công việc này dựa trên tập những luật được định nghĩa trước miêu tả một hành động tấn công. Tất cả những sự kiện liên quan tới an ninh tồn tại trong dấu vết nhật ký là được dịch sang một luật theo kiểu nếu-thì-không-thì (If-then-else).

Phân tích dấu hiệu: Tương tự hệ chuyên gia, nguyên lý này dựa trên những kiến thức về các hành động tấn công. Chúng chuyển các miêu tả về mặt ngữ nghĩa các hành động tấn công sang định dạng dấu vết. Vì thế tín hiệu tấn công có thể được tìm thấy trong nhật ký hay dữ liệu vào của dòng dữ liệu. Một kịch bản tấn công có thể được miêu tả như là chuỗi các sự kiện do hành động tấn công tạo ra hoặc tìm thấy được trong nhật ký. Nguyên lý này sử

dụng tính tương đương với dữ liệu ghi trong nhật ký. Quá trình dò tìm sử dụng cơ chế tìm chuỗi thông thường. Nói chung kỹ thuật này hoạt động rất hiệu quả và thường được sử dụng trong các sản phẩm thương mại.

Phân tích dịch chuyển trạng thái: Ở đây một hành động tấn công được miiêu tả là một tập các mục tiêu và sự dịch chuyển cần đạt được từ những kẻ xâm nhập hệ thống để làm phá hoại hệ thống. Các dịch chuyển sẽ được biểu diễn bằng biểu đồ trạng thái.

Phương pháp phân tích thống kê: Đây là kỹ thuật thường được sử dụng nhất. Những hành động của người sử dụng trên hệ thống được kiểm tra bởi một số biến theo thời gian. Nếu một hành động không tuân theo những dữ liệu đã có sẵn, hành động đó có thể bị coi là xâm nhập không hợp lệ. Ví dụ một số biến như số lần đăng nhập, thoát; số lần truy nhập tập tin trong một khoản thời gian; phần trăm sử dụng CPU… Hệ thống sẽ lưu giữ giá trị cho mỗi biến, giá trị này được sử dụng để dò tìm những giá trị mới vượt quá ngưỡng cho phép. Phương pháp này dựa vào việc tìm kiếm dữ liệu của người dùng được tập hợp theo nhóm các biến cũng không đạt được hiểu quả cao. Vì thế một mô hình phức tạp về các hoạt động của người dùng được phát triển sử dụng thuật ngữ profile người dùng. Những profile này được cập nhật thường xuyên để giữ được sự thay đổi trong hành động của người sử dụng. Lý thuyết về thống kê được thường xuyên sử dụng để xây dựng hệ thống IDS dựa trên các profile về hành động của người dùng.

Mạng Nơron: Sử dụng nguyên lý mạng nơron về mối quan hệ đầu vào và đầu ra vector và tổng hợp chúng để đưa ra mối quan hệ vào/ra mới. Với mạng nơron, để dò tìm xâm nhập, mục đích chính là học hành động của diễn viên trong hệ thống. Nó được biết đến là lý thuyết thống kê cục bộ tương đương mạng nơron. Lợi điểm của việc sử dụng mạng nơron thông qua thống kê tập trung là việc có một cách đơn giản để biểu diễn quan hệ không tuyến tính giữa các biến và học được quan hệ đó được một cách tự động. Thí nghiệm được tiến hành với mạng nơron dự đoán hành động của tài khoản có quyền cao nhất trên hệ thống (Super-User). Từ kết quả đó, chúng ta có thể nhận thấy rằng hành động của tài

khoản (Super-User) đó trên mạng là có thể dự đoán được (bởi vì các tiến trình tự động của hệ thống là bình thường). Có một số ngoại lệ còn hầu hết hành động của người dùng thường trên mạng là dự đoán được. Mạng nơron vẫn là một kỹ thuật đòi hỏi thuật toán chuyên sâu và chưa dược dùng rộng rãi.

Xác định mục đích sử dụng: Kỹ thuật này mô hình hóa hành động của người dùng bởi một tập những nhiệm vụ mức cao. Chúng phải hoạt động trên hệ thống. Những nhiệm vụ này là một loạt những hoạt động mà lần lượt phải phù hợp với dữ liệu thích hợp được kiểm tra. Bộ phân tích giữ một tập những nhiệm vụ được chấp nhận bởi mỗi người sử dụng. Bất kỳ một sai lệch nào đều sinh ra một cảnh báo.

Miễn dịch máy tính: Tương tự hệ miễn dịch dẫn tới sự phát triển của một kỹ thuật mà dựa trên một mô hình những hoạt dộng thông thường của dịch vụ mạng, hơn là với từng người sử dụng độc lập. Mô hình này chứa một chuỗi những lời gọi ngắn được tạo bởi các tiến trình. Hoạt động tấn công lợi dụng thiếu sót của mã nguồn ứng dụng cũng giống như thực hiện theo cách không thông thường. Đầu tiên, một tập những dữ liệu tham chiếu được thu thập mà nó biểu diễn những hành động phù hợp của dịch vụ. Khi kiến thức này được thêm vào với chuỗi biết trước các lời gọi hệ thống. Những mẫu này là được dùng để thường xuyên theo dõi những lời gọi hệ thống, kiểm tra khi nào chuỗi được phát ra là liệt kê trong những cơ sở có sẵn, nếu không có thì một tín hiệu cảnh báo được đưa ra. Kỹ thuật này có một lợi điểm là rất ít cảnh báo sai, nếu cơ sở kiến thức là đúng. Hạn chế của nó là không có khả năng dò tìm lỗi trong chương trình của dịch vụ mạng. Khi một kẻ tấn công sử dụng những hành động phù hợp trên hệ thống có thể đạt dược quyền truy nhập mà không có xảy ra cảnh báo.

Máy tự học(learning machine): Đây là kỹ thuật của trí tuệ nhân tạo dùng lưu giữ dòng dữ liệu người dùng. Nhập vào các câu lệnh theo mẫu vector và dùng như tham chiếu của profile của người dùng. Các profile được nhóm lại thành các thư viện theo các câu lệnh có đặc điểm tương đồng, giống nhau.

Tối ưu dữ liệu(data mining): Nhìn chung là một kỹ thuật tổng hợp của các kỹ thuật, dùng công cụ lọc những điều chưa biết, nhưng là dữ liệu có ích từ một

lượng dữ liệu lớn. Nguyên lý tối ưu hóa dữ liệu là xắp sếp, phân chia ở quá trình xử lý lượng dữ liệu lớn. tuy nhiên nguyên lý này không có ích lắm khi dùng để phân tích lưu lượng mạng. Một chức năng của kỹ thuật tối ưu được dùng trong dò tìm tấn công là cây quyết định. Mô hình cây quyết định cho phép một người dùng có thể dò tìm sự bất thường trong một lượng dữ liệu lớn. Một kỹ thuật khác cần quan tâm là phân mảnh, cho phép phân tích một mẫu của hành động tấn công. Điều này được thực hiện bằng cách tìm những mẫu phù hợp được trích từ tập các bản ghi nhật ký có sự tham chiếu tới lượng lớn dữ liệu chưa biết. Một kỹ thuật tối ưu hóa dữ liệu kết hợp với việc tìm một luật kết hợp, nó cho phép một người trích những kiến thức chưa biết trên những tấn công mới hoặc xây dựng dựa trên mẫu hành động thông thường. Dò tìm bất thường hay tạo ra những báo động sai. Với tối ưu hóa dữ liệu chúng ta dễ dàng có được tương quan giữa dữ liệu liên quan cảnh báo và dữ liệu nhật ký, nhờ đó có thể giảm được những thông báo sai cần quan tâm.

CHƯƠNG IV: XÂY DỰNG HỆ THỐNG IDS CHO MẠNG LAN

Như trên ta đã thấy, an ninh an toàn mạng máy tính có thể bị đe dọa tới rất nhiều góc độ và nguyên nhân khác nhau. Đe dọa an ninh có thể xuất phát từ bên ngoài mạng nội bộ hoặc cũng có thể xuất phát từ ngay bên trong tổ chức, do đó để đảm bảo anh ninh an toàn mạng máy tính cần có nhiều giải pháp cụ thể khác nhau. Tuy nhiên tổng quan nhất có 3 giải pháp cơ bản sau:

- Giải pháp phần cứng
- Giải pháp phần mềm
- Giải pháp con người

Trong phạm vi nghiên cứu của đề tài này sẽ đi sâu vào bảo mật hệ thống mạng Lan bằng Cisco IDS phần cứng với những ưu việt sau:

- Các tính năng phát hiện chính xác làm giảm đáng kể các cảnh báo sai
- Khả năng nâng cấp hoạt động kinh doanh cũng như các sản phẩm của Cisco
- Hệ thống phát hiện xâm phạm thời gian thực báo cáo và ngăn chặn các hành động trái phép
- Việc phát hiện được thực hiện ở nhiều mức khác nhau
- Khả năng hoạt động ổn định cho hiệu suất cao
- Quản lý các danh sách truy cập động, thích nghi kịp thời với hành vi của kẻ xâm nhập
- Quản lý GUI tập trung

4.1. Mục tiêu xây dựng hệ thống

Song song với việc xây dựng nền tảng công nghệ thông tin cũng như phát triển các ứng dụng máy tính trong sản xuất kinh doanh khoa học giáo dục xã hội, thì việc bảo vệ những thành quả đó là việc không thể thiếu. Sử dụng các bức tường lửa (Firewall) để bảo vệ mạng nội bộ Intranet tránh sự tấn công bên ngoài là một giải pháp hữu hiệu đảm bảo được các yếu tố:

- An toàn cho hoạt động của toàn bộ hệ thống mạng
- Bảo mật trên nhiều phương diện
- Khả năng kiểm soát cao
- Đảm bảo tốc độ nhanh, mềm dẻo và dễ sử dụng
- Trong suốt với người sử dụng
- Đảm bảo kiến trúc mở

Trên đây là các giải pháp bảo mật mạng nội bộ với luồng truy cập từ bên ngoài vào trong. Đối với việc kiểm soát truy cập từ bên trong mạng nội bộ thì sẽ khó kiểm soát hơn vì các chính sách truy cập áp dụng trên từng người dùng không được siết chặt. Giải pháp cho vấn đề này là làm sao kiểm soát được các hoạt động truy cập mạng ra bên ngoài và truy cập tài nguyên bên trong. Với Cisco IDS thì việc kiểm soát bên trong mạng nội bộ sẽ trở nên dễ dàng hơn, giúp người quản trị có thể làm chủ hệ thống, ngăn ngừa các nguy cơ tấn công mạng, chủ động trong việc phòng thủ hệ thống….

4.2. Cấu trúc hệ thống

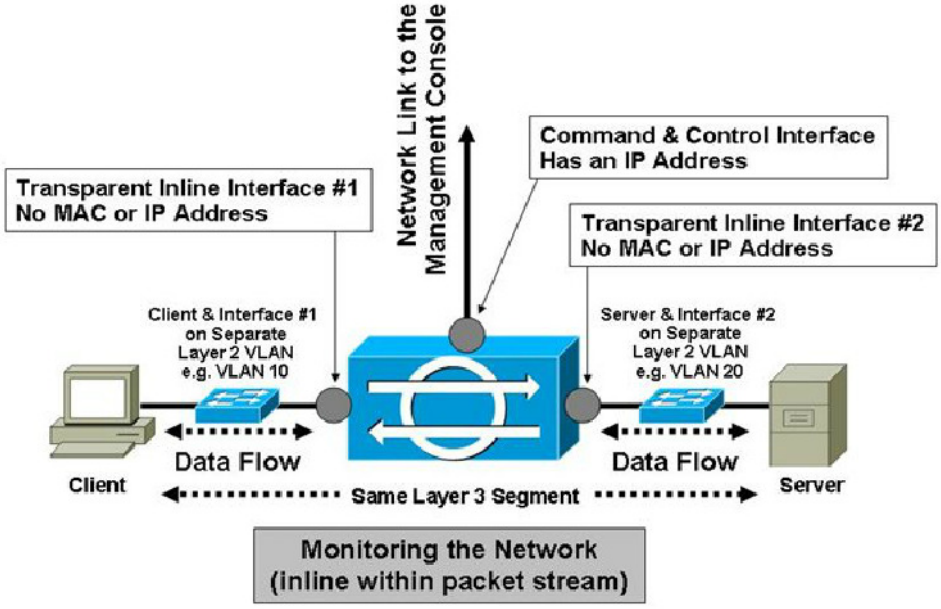
Để đảm bảo mạng hoạt động ổn định và tin cậy, nhiều giải pháp an ninh đã được thực hiện như thiết lập hệ thống firewall, thiết lập các cơ chế xác thực, mã hóa, xây dựng các mạng VPN… Tuy nhiên những hệ thống an ninh này chưa có khả năng phát hiện và chống lại những xâm nhập, tấn công mới. Vì thế nhu cầu đặt ra là phải thiết lập được một hệ thống cảnh báo sớm những tấn công có thể hoặc

đang xảy ra. Mục tiêu của phần này là xây dưng một hệ thống phát hiện xâm nhập cho mạng nội bộ. Qúa trình triển khai được chia làm hai giai đoạn (hai pha):

- Xây dựng hệ thống IDS cho các hệ thống máy chủ dịch vụ, bao gồm hệ thống máy chủ cho dịch vụ tên miền DNS, WebServer, FTP Server…

- Xây dựng hệ thống cho các thiết bị mạng, thiết lập các hệ thống thu thập thông tin (Sensor) cho các vùng lưu lượng mạng kết hợp với hệ thống cho máy chủ tạo thành một hệ thống cho toàn mạng

Mô hình tổng quan khi triển khai IDS về chức năng được thiết kế như sau



Hình 4.1 – Mô hình tổng quan khi triển khai IDS về chức năng

Mô hình này có những lợi ích sau:

- Giám sát được toàn bộ hệ thống mạng với Inline mode

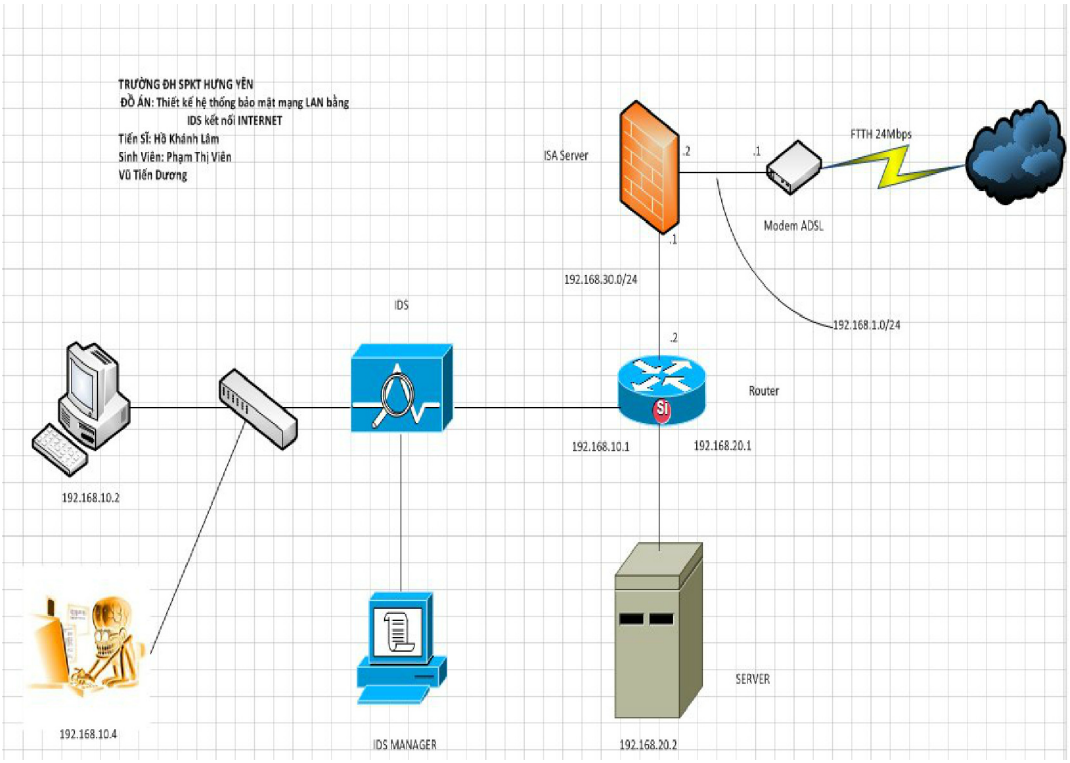
- Tách biệt interface quản lý nâng cao độ bảo mật IDS không bị xâm phạm

- Trong suốt với người sử dụng

Đặc tính:

- Hai cặp interface inline không có địa chỉ IP, địa chỉ MAC
- Cùng layer 3 segment
- Truyền thông giữa các VLAN

Mô hình hệ thống mạng Lan bảo mật được thiết kế như sau:



Hình 4.2 – Mô hình tổng quan hệ thống

Hệ thống bao gồm:

- ***Isa server 2006 bảo mật toàn bộ hệ thống mạng Lan***

- Quản lý băng thông với từng Vlan
- Làm chức năng Proxy server, caching web

- ***Switch layer3***

Phân chia và định tuyến các Vlan

- ***Server***

Làm web server và FTP server, DNS server

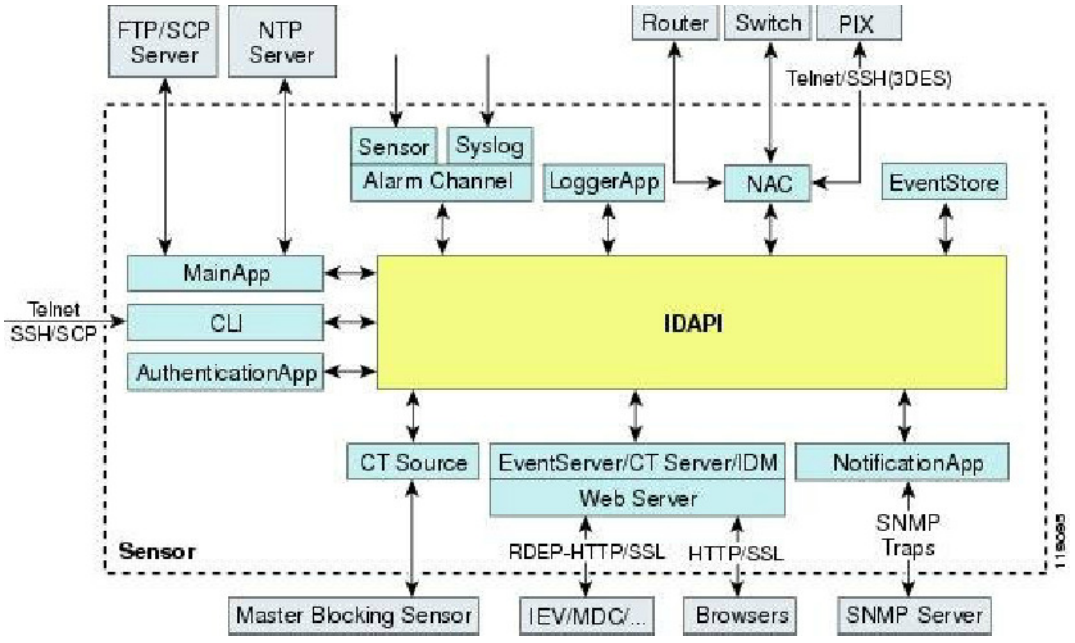
- ***Cisco IDS***

Cung cấp việc giám sát và bảo vệ mạng nội bộ

- ***PC attacker***

Cài Window XP, Cain & Abel, Nmap, Wireshark, máy ảo BackTrack 5

4.3. Tổng quan các thành phần Cisco IDS



Hình 4.3 – Các thành phần Cisco IDS

Chúng ta có thể cài đặt CISCO IDS trên hai nên tảng: nền tảng thiết bị và nền tảng module gắn thêm. Điểm đặc biệt của Cisco IDS là chạy trên nền Linux. Cisco đã bảo mật gần như tuyệt đối hệ điều hành này bằng cách bỏ đi các gói phần mềm,

các dịch vụ không cần thiết, hạn chế việc truy cập mạng và ngăn ngừa khả năng truy cập vào shell linux.

Cisco IDS bao gồm các thành phần sau:

- MainApp: Khởi động hệ điều hành, bật và tắt các ứng dụng khác, cấu hình hệ điều hành và thực hiện nâng cấp. Nó chứa các thành phần sau:

- CtlTransSource (Control Transaction Server): Cho phép sensor gửi các giao dịch điều khiển.

- Event Store: Được dùng để lưu trữ các sự kiện (lỗi, tình trang, và các tin cánh báo hệ thống). Event Store có thể truy cập thông qua CLI, IDM, ASDM, hay RDEP

- InterfaceApp: Cấu hình bypass và thiết lập các interface vật lý, định nghĩa các cặp interface. Trong đó có việc thiết lập tốc độ, duplex và trạng thái quản trị

- LogApp: Ghi lại tất cả các sự kiện của ứng dụng gửi đến Event Store

- Attack Response Controller (được hiểu như là bộ điều khiển truy cập mạng): Quản trị các thiết bị mạng ở xa như firewall, router và switch để cung cấp các cơ chế ngăn ngừa khi một sự kiện xay ra. ARC tạo và áp dụng các ACL trên các thiết bị mạng được Cisco IDS quản lý

- NotificationApp: Gửi SNMP traps khi tạo ra một sự kiện.

- Web Server (HTTP RDEP2 server): Cung cấp người dùng giao diện web và giao tiếp với các thiết bị IDS khác thông qua RDEP2

- AuthenticationApp: Cấp quyền cho người dùng thực hiện quản lý CLI, IDM, ASDM

- SensorApp (Anlysis Engine): Thực hiện bắt gói tin và phân tích