BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

ISO 9001:2008

TRẦN THỊ HẰNG

LUẬN VĂN THẠC SĨ
NGÀNH HỆ THỐNG THÔNG TIN

HẢI PHÒNG, 2016

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

TRẦN THỊ HẰNG

NGHIÊN CỨU TÌM HIỂU THỰC TRẠNG VỀ AN NINH MẠNG VÀ BIỆN PHÁP KHẮC PHỤC

LUẬN VĂN THẠC SĨ
NGÀNH CÔNG NGHỆ THÔNG TIN

CHUYÊN NGÀNH: HỆ THỐNG THÔNG TIN
MÃ SỐ: 60 48 01 04

NGƯỜI HƯỚNG DẪN KHOA HỌC:
TS. Hồ Văn Canh

Hải Phòng - 2016

MỤC LỤC

BẢNG KÝ HIỆU VIẾT TẮT

Ký hiệu	Dạng đầy đủ
SELinux	Security Enhanced Linux
DAC	Discretionary Access Control
MAC	Mandatory Access Control
RBAC	Role Based Access Control
TE	Type Enforcement
LSM	Linux Security Module
MLS	Multi Level Security
NSA	National System Agent
AVC	Access Vector Cache
PSL	Polgen Specification Language
RHEL	Red Hat Enterprise Linux
RMP	Role Mining Problem
HĐH	Hệ điều hành
SS7	Sigmalling System No 7
CCSS7	Cammar channel Interottice signaliry 7
VENOM	Virtual Envionment Neglected Operations ..
CTTT	Chiến Tranh Thông Tin.
PKI	Public Key Infrastructure - Cơ sở hạ tầng khóa công khai.
IDS	Intrusion Detection System - Hệ thống phát hiện xâm nhập (tái phép).

LỜI CẢM ƠN

Đầu tiên em xin gửi lời cảm ơn chân thành tới các thầy, các cô trường Đại học Dân Lập Hải Phòng đã nhiệt tình giảng dạy và truyền đạt kiến thức cho em trong thời gian học tập tại trường.

Em xin gửi lời cảm ơn sâu sắc tới thầy Hồ Văn Canh, người đã định hướng, hướng dẫn và hỗ trợ em rất nhiều để hoàn thành luận văn này.

Em xin gửi lời cảm ơn các anh chị đồng nghiệp và cảm ơn bạn bè cùng khoá, cùng trường đã nhiệt tình hỗ trợ trong thời gian làm luận văn.

Mặc dù đã rất cố gắng hoàn thành luận văn này, xong luận văn sẽ khó tránh khỏi những thiếu sót. Em rất mong nhận được sự nhận xét, góp ý, tận tình chỉ bảo từ các thầy, cô.

Một lần nữa, em xin chân thành cảm ơn tất cả mọi người!

LỜI CAM ĐOAN

Tôi xin cam đoan bản Luận văn này là công trình nghiên cứu khoa học độc lập của tôi. Luận văn này không sao chép toàn bộ các tài liệu, công trình nghiên cứu của người khác. Tất cả các đoạn trích dẫn nằm trong các tài liệu, công trình nghiên cứu của người khác đều được ghi rõ nguồn và chỉ rõ trong tài liệu tham khảo.

Tôi xin cam đoan những điều trên là đúng sự thật, nếu sai, tôi xin hoàn toàn chịu trách nhiệm.

TÁC GIẢ LUẬN VĂN

Trần Thị Hằng

LỜI MỞ ĐẦU

Ngày nay, với sự phát triển mạnh mẽ của Công nghệ Thông tin, việc sử dụng thông tin trên mạng Internet ngày càng được mở rộng và hiệu quả trên tất cả các ngành nghề, các lĩnh vực. Tuy nhiên, bên cạnh đó người sử dụng cũng phải đối mặt với những nguy cơ mất mát, rò rỉ thông tin, bị xâm hại các quyền riêng tư khi truy cập mạng. Đây là một trong những lý do khiến người sử dụng lo ngại, đặc biệt là các cơ quan nhà nước.

Theo số liệu thống kê năm 2011 của BKAV, có 64,2 triệu lượt máy tính tại Việt Nam bị nhiễm virus, 38.961 dòng virus xuất hiện mới, 2.245 website của các cơ quan, doanh nghiệp tại Việt Nam bị tấn công, hơn 85.000 máy tính tại Việt Nam bị cài virus Ramnit để lấy cắp dữ liệu quan trọng.

Đối với các công ty lớn, nguy cơ bị tấn công vào hệ thống đồng nghĩa với việc họ sẽ bị thiệt hại hàng tỷ USD, uy tín trước khách hàng bị giảm sút. Với các cơ quan y tế và quốc phòng thì thiệt hại còn có thể thảm khốc hơn gấp nhiều lần.

Với nguồn tài nguyên thông tin phong phú, đa dạng, hấp dẫn trên mạng chính là sự tiềm ẩn của loại hình chiến tranh mới: “Chiến tranh thông tin”.

Trong lĩnh vực An ninh Quốc phòng, môi trường thông tin mở trên mạng đã đặt ra những thách thức gay gắt đối với chúng ta. Một mặt ta phải tổ chức khai thác một cách có hiệu quả và bảo vệ nguồn tài nguyên thông tin Quốc gia, mặt khác ta cần phải chiếm được ưu thế và đánh bại đối phương bằng các đòn tấn công thông tin qua mạng Internet khi cần thiết.

Theo báo Dân Việt ngày 14/06/2011, trong hơn một tuần có hàng trăm website Việt Nam đã bị hacker tấn công, trong đó có khá nhiều vụ tấn công tin tặc để lại thông điệp bằng tiếng Trung hoặc cả hình ảnh cờ Trung Quốc.

Điều này cho thấy hình thái chiến tranh thông tin đã và đang dần dần hình thành ở Việt Nam. Vấn đề an toàn thông tin cho mạng máy tính và việc

nghiên cứu về chiến tranh thông tin trên mạng và giải pháp phòng tránh, đánh trả cụ thể là một nhu cầu cấp bách hiện nay.

Do đó, "Tấn công – Phòng thủ" trên mạng Internet là một trong những bài toán cần phải được đặt ra hàng đầu trong lĩnh vực An ninh Quốc phòng ngày nay. Vì vậy, tôi đã chọn đề tài: "**Nghiên cứu tìm hiểu thực trạng về an ninh mạng và biện pháp đối phó**" cho luận văn tốt nghiệp của mình.

Các nội dung nghiên cứu trong luận văn gồm những vấn đề sau:

-Thực trạng của vấn đề tấn công và phòng thủ trên mạng Internet.

-Một số dạng phá hoại trong chiến tranh thông tin trên mạng máy tính và dự báo một số dạng phá hoại mới.

-Vấn đề tấn công – phòng thủ mạng. Đề xuất giải pháp cho vấn đề tấn công – phòng thủ mạng.

-Xây dựng mô hình thử nghiệm cho một giải pháp tấn công – phòng thủ mạng.

Chiến tranh thông tin có quy mô rất lớn, nhằm vào nhiều lĩnh vực, khía cạnh, có phạm vi ảnh hưởng sâu rộng. Trong đề tài này, tôi tập trung về các cách thức và cách phòng chống các hoạt động ác ý làm ảnh hưởng đến thông tin trên mạng. Nghiên cứu xây dựng thử nghiệm một công cụ trinh sát, tấn công và phòng thủ trên mạng.

Do còn nhiều hạn chế về thời gian và tài liệu nên đề tài còn nhiều thiếu sót. Rất mong nhận được sự đóng góp của các thầy cô và các bạn để đề tài được hoàn thiện hơn.

Tôi xin chân thành cảm ơn!

Chương 1: TÌNH HÌNH AN NINH AN TOÀN MẠNG MÁY TÍNH TẠI VIỆT NAM

1.1. Thực trạng an ninh mạng tại Việt Nam

Internet ngày càng phát triển mạnh mẽ và có sức ảnh hưởng rộng rãi tới tất cả các ngành nghề, các lĩnh vực của cuộc sống. Hiện nay, Internet đã trở thành một môi trường phức tạp, bao hàm mọi thành phần xã hội. Con người sử dụng Internet với nhiều mục đích khác nhau, trong đó có một số người tận dụng khả năng truyền bá thông tin nhanh chóng để phát tán những tin tức, sự kiện với mục đích làm phương hại đến tên tuổi, uy tin của một cá nhân, tổ chức hay đến sự ổn định một quốc gia nhằm mục đích chính trị.

Mạng máy tính cũng sinh ra một tầng lớp người mới – những tay hacker. Đây là những người nói chung có niềm đam mê rất lớn đối với máy tính, với công nghệ thông tin. Sự đam mê khiến họ trở thành những kẻ luôn luôn tò mò, tìm cách mổ xẻ, khám phá mọi điều liên quan đến Tin học. Trong quá trình đó họ phát hiện các hệ thống thông tin đó có thể bị tấn công. Từ lúc này, giới hacker chia thành hai phái: phái thứ nhất chủ trương nghiên cứu, khám phá để báo cho các nhà quản trị hệ thống thông tin biết, tìm cách phòng ngừa, sửa chữa, khắc phục nhằm bảo vệ cho hệ thống – đó là các hacker mũ trắng (white-hat hacker). Phái thứ hai muốn nhân đó để tấn công hệ thống, lấy cắp thông tin, tiền bạc hay thậm chí chỉ để ghi lại tên tuổi của mình cho nổi tiếng – đó là các hacker mũ đen (black-hat hacker). Loại hacker mũ đen này hết sức nguy hiểm do trình độ cao kèm theo mục đích đen tối của chúng.

Phần lớn các cuộc tấn công trên mạng được thực hiện thông qua việc sử dụng một hoặc nhiều công cụ phần mềm (do người tấn công tự xây dựng hoặc có được từ các nguồn khác nhau). Trong bản luận văn này, những phần mềm đó được gọi là các phần mềm phá hoại.

Phần mềm phá hoại là những phần mềm được thiết kế, xây nhựng nhằm mục đích tấn công gây tổn thất hay chiếm dụng bất hợp pháp tài nguyên của máy tính mục tiêu (máy tính bị tấn công). Những phần mềm này thường được che dấu hay hoá trang như là phần mềm hợp lệ, công khai hoặc bí mật thâm nhập vào máy tính mục tiêu.

Những phần mềm phá hoại khác nhau có phương thức và nguy cơ gây hại khác nhau.

Các vụ tấn công trên mạng ngày càng gia tăng cả về qui mô và tính chất nguy hiểm. Có thể kể ra một số vụ tấn công như sau:

Tình hình an ninh mạng năm 2010

Năm 2010 thực sự là năm nóng bỏng với vấn đề an ninh mạng. Sự phát triển của tội phạm mạng đang diễn ra với tốc độ nhanh hơn bao giờ hết cả về quy mô, tính chuyên nghiệp, trình độ kỹ thuật và tiềm lực tài chính. Điều đáng báo động là sự phá hoại của virus máy tính không còn đơn thuần là chứng tỏ khả năng hay chuộc lợi cá nhân mà đã chuyển hướng sang hạ tầng công nghiệp Quốc gia.

Vụ việc website báo điện tử bị tấn công là một trong những sự kiện an ninh mạng gây chú ý nhất trong năm 2010. Theo thống kê của các cơ quan an ninh mạng, đã có hàng ngàn website lớn tại Việt Nam bị virus xâm nhập, lộ thông tin quan trọng hay bị tấn công từ chối dịch vụ. Trong đó nổi lên là những cuộc tấn công liên tục vào báo điện tử VietNamNet trong một thời gian dài với nhiều hình thức khác nhau. Hơn 1000 website lớn tại Việt Nam như VietNamNet đã bị tấn công năm 2010 với các hình thức tấn công đa dạng từ thay đổi giao diện, đánh cắp các dữ liệu nhạy cảm trong website và tấn công làm tê liệt hệ thống website đó. Đó có thể là các website của các ngân hàng, các tổ chức về vận tải, các tập đoàn lớn, các sở, ban, ngành,… (Chương trình cuộc sống số trên kênh VTV1 ngày 12/02/2011).

Theo sự thống kê của Bkis, năm 2010 đã có 58,6 triệu lượt máy tính tại Việt Nam bị nhiễm virus, 57.835 dòng virus mới xuất hiện, với hơn 1000 website bị hacker tấn công.

Bkav tổng kết tình hình an ninh mạng năm 2010:

- Bùng nổ phần mền diệt virus giả mạo – Fake AV

Năm 2010 đã chứng kiến sự bùng nổ lượng máy tính bị nhiễm virus giả mạo phần mềm diệt virus, lên đến 2,2 triệu lượt, gấp 8,5 lần so với con số 258.000 của năm 2009.

Phần mềm giả mạo dụ người dùng tới các website giả mạo quét virus trực tuyến, nhằm cài đặt mã độc lên máy tính là đặc điểm chung của các FakeAV. Nguyên nhân chính khiến rất nhiều người sử dụng tại Việt Nam đã nhiễm loại virus này là do thói quen dùng phần mềm trôi nổi, không có bản quyền.

- Giả mạo file dữ liệu, xu hướng mới của virus

Hơn 1,4 triệu lượt máy tính đã bị nhiễm dòng virus giả mạo thư mục, giả mạo file ảnh, file word, file excel…

Bằng cách sử dụng icon để nguỵ trang, file thực thi của virus trông có vẻ giống hệt một thư mục hay một file dữ liệu dạng ảnh, file word, file excel… Điều này đã dễ dàng đánh lừa cảm quan của người sử dụng, thậm chí là cả các chuyên gia có kinh nghiệm, khiến họ dễ dàng mở file virus và bị nhiễm mà không chút nghi ngờ. Đây cũng là lý do khiến dòng virus này tuy mới xuất hiện nhưng đã lan truyền với tốc độ chóng mặt.

- Virus phá huỷ quay trở lại

Tuy chưa gây hậu quả nghiêm trọng trên diện rộng, nhưng sự quay trở lại của virus phá huỷ dữ liệu W32.Delfile.Worm, W32.FakeStuxer.Trojan sẽ là mối đe doạ lớn của người sử dụng trong thời gian tới.

Với xu hướng tập trung nhiều dữ liệu quan trọng trên máy tính như hiện nay, virus phá huỷ dữ liệu quay trở lại với tốc độ lây lan nhanh chóng sẽ gây ra những hậu quả khôn lường khi lây lan trên diện rộng.

- Phát tán virus để xâm nhập hệ thống, tấn công DDoS

Liên tiếp nhiều website lớn tại Việt Nam bị virus xâm nhập, lộ thông tin quan trọng hay bị tấn công DDoS trong thời gian qua đang là vấn đề gây lo lắng trong xã hội.

Bkav đã phát hiện một số nhóm hacker đã cài đặt virus xâm nhập vào các hệ thống mạng tại Việt Nam, qua đó đánh cắp thông tin bí mật nội bộ của các tổ chức. Bên cạnh đó chúng còn kiểm soát được các website chuyên download phần mềm nhằm cài đặt virus vào các máy tính tải phần mềm từ các website này.Từ đó chúng có thể điều khiển mạng lưới máy tính ma – botnet – để tấn công DDoS vào các hệ thống lớn tại Việt Nam. Đây là tình trạng đáng báo động vì ngoài việc các hệ thống lớn có thể bị tấn công bất cứ lúc nào, còn có hàng chục nghìn máy tính trên cả nước đang bị hacker điều khiển.

Tình hình an ninh mạng năm 2011

Tổng kết tình hình virus và an ninh mạng từ Hệ thống giám sát virus của Bkav, năm 2011 đã có 64,2 triệu lượt máy tính bị nhiễm virus, 38.961 dòng virus mới xuất hiện, trong đó lây lan nhiều nhất là virus W32.Sality.PE. Virus này đã lây nhiễm trên 4,2 triệu lượt máy tính. Ngoài ra, năm 2011 còn có 2.245 website của các cơ quan doanh nghiệp tại Việt Nam bị tấn công.

Lừa đảo trực tuyến gia tăng trên mạng xã hội. Trung bình mỗi tháng Bkav nhận được hơn 30 báo cáo về lừa đảo qua Yahoo Messenger. Trong mỗi vụ số nạn nhân có thể lên tới hàng chục người. Mặc dù đã được cảnh báo nhiều lần nhưng do sự nhẹ dạ của người sử dụng mà các vụ cướp nick hoặc lừa tiền vẫn diễn ra liên tiếp.

Không chỉ Yahoo mà cả Facebook, mạng xã hội lớn nhất thế giới đã trở thành phương tiện để tin tặc lợi dụng với hàng loạt những vụ giả mạo người nổi tiếng để lừa đảo.Mạng xã hội và chát trực tuyến đang trở thành công cụ đắc lực của tin tặc.

Năm 2011 cũng là năm của các cuộc tấn công mạng. Liên tiếp xảy ra các cuộc tấn công với các hình thức khác nhau vào hệ thống của các tổ chức doanh nghiệp Việt Nam. Có những cuộc tấn công xâm nhập trái phép, phá hoại cơ sở dữ liệu hoặc deface các website. Cũng có những cuộc tấn công DDoS làm tê liệt hệ thống trong thời gian dài, tấn công cướp tên miền của các doanh nghiệp diễn ra liên tiếp. Nguy hiểm hơn, đã xuất hiên các cuộc tấn công âm thầm, cài đặt các virus gián điệp đánh cắp tài liệu của các cơ quan quan trọng.

Đáng chú ý trong năm 2011 là sự việc hơn 85.000 máy tính tại Việt Nam bị cài virus Ramnit để lấy cắp dữ liệu quan trọng. Điều này cho thấy các cuộc tấn công còn có thể gây ảnh hưởng tới an ninh quốc gia.

Tình hình an ninh mạng năm 2012 đến nay

Theo dự đoán của Bkav, năm 2012 sẽ tiếp tục chứng kiến sự bùng nổ của virus trên điện thoại di động. virus siêu đa hình tiếp tục lây lan rộng, nhiều cư dân mạng sẽ tiếp tục bị lừa đảo trực tuyến, tấn công mạng không chỉ là vấn đề của Việt Nam, mà là vấn đề của cả thế giới.

Lỗ hổng tràn lan trên các website .gov.vn. Theo nghiên cứu của Hiệp hội an toàn thông tin Việt Nam (VNISA) phát hiện 3697 lỗi trong 100 website .gov.vn, trong đó 489 lỗi thuộc diện nghiêm trọng, 396 lỗi ở mức cao, còn lại 2812 lỗi ở mức trung bình/yếu. 80% website được khảo sát không có biện pháp bảo mật tối thiểu. Kết quả nghiên cứu này được đưa ra trong hội thảo "Xây dựng chính sách đảm bảo ATTT trong phát triển chính phủ điện tử tại Việt Nam" diễn ra ngày 25/05/2012 tại Hà Nội.

Theo thống kê của hãng bảo mật Kasperspy, Việt Nam đứng số 1 thế giới về tỷ lệ lây nhiễm mã độc qua thiết bị lưu trữ ngoài (USB, thẻ nhớ, ổ cứng di động) với tỷ lệ 70,83% máy tính bị lây nhiễm; 39,95% người dùng phải đối mặt với mã độc bắt nguồn từ không gian mạng.

Thống kê trong năm 2015 có hơn 10.000 trang (hoặc cổng) thông tin điện tử có tên miền .vn bị tấn công, chiếm quyền điều khiển, thay đổi giao diện, cài mã độc (tăng 68% so với năm 2014), trong đó có 224 trang thuộc quản- lý của các cơ quan nhà nước (giảm 11% so với năm 2014).

Các cổng Thông tin điện tử (TTĐT) Việt Nam cũng không được quan tâm, đầu tư về bảo mật tiếp tục là mục tiêu của tin tặc. Thống kê trong năm 2015 có hơn 10.000 trang (hoặc cổng) thông tin điện tử có tên miền .vn bị tấn công, chiếm quyền điều khiển, thay đổi giao diện, cài mã độc (tăng 68% so với năm 2014), trong đó có 224 trang thuộc quản lý của các cơ quan nhà nước (giảm 11% so với năm 2014).

Thời gian tin tặc tấn công vào hệ thống trang tin/cổng TTĐT của Việt Nam nhiều nhất là tháng 6-2015 với số lượng các trang tin bị tấn công lên đến hon 1.700 trang, trong đó có 56 trang tên miền .gov.vn. Có 24 bộ/ngành, 48 tỉnh/thành phố, 13 trường đại học, cao đẳng bị tin tặc tấn công. Gần đây nhất là vào ngày 28-29/8/2016, Tin tặc đã tấn công và làm tê liệt nhiều giờ liền tại Trung tâm điều khiển của Hãng hàng không tại sân bay Tân Sơn Nhất và Nội Bài, làm thiệt hại lớn về kinh tế và gây bức xúc trong dư luận.

Bên cạnh việc khai thác các lỗ hổng bảo mật trên các hệ điều hành và hệ thống mạng để tấn công xâm nhập, tin tặc còn sử dụng chính các tài liệu, văn bản do một số cơ quan, đơn vị của Việt Nam soạn thảo mà chúng đã đánh cắp được hoặc sử dụng thông tin, tài liệu đăng tải trên các trang mạng phản động làm mồi để phát tán mã độc, xâm nhập hệ thống mạng của các cơ quan trọng yếu khác của Việt Nam. Đặc biệt gần đây nhất, theo[14], ngày 28-29

tháng 8 năm 2016, các websides của Cục hàng không dân dụng Việt Nam (Vietnam-airlines) dã bị tấn công làm cho hệ thống điều khiển sân bay Tân Sơn Nhất và sân bay Nội Bài bị tê liệt trong nhiều giờ, các máy bay đi và đến không thể cất và hạ cánh được, gây tổn thất hàng chục tỷ đồng VNĐ.

Các nước trên thế giới cũng liên tục phát hiện các vụ tấn công, xâm nhập vào hệ thống máy tính của các cơ quan chính phủ, tổ chức chính tri, các ngành công nghiệp, kinh tế mũi nhọn, các hãng hàng không lớn, cơ quan truyền thông, tổ chúc y tế, giáo dục... nhằm phá hoại, đánh cắp dữ liệu, thu thập thông tin tình bảo liên quan đến chính sách về kinh tế, chính trị, an ninh, quốc phòng và đối ngoại.

Nổi lên là các vụ tấn công vào hệ thống thư điện tử của Bộ Ngoại giao, hệ thống máy tính của Nhà Trắng, Cơ quan quản lý nhân sự Chính phủ Mỹ...

Nhiều nhóm tin tặc tấn công bằng mã độc để đánh cắp dữ liệu, thu thập thông tin tình báo quan trọng về chính trị, kinh tế, quân sự. Đối tượng chính là các cơ quan chính phủ, các tổ chức kinh tế, các cơ quan báo chí của hầu hết các nước trên thế giới đặc biệt là khu vực Châu Á và Đông Nam Á như Malaysia, Thái Lan, Ấn Độ, Hàn Quốc, Nhật Bản...

Trong thời gian gần đây, các loại tội phạm công nghệ cao tại Việt Nam phát triển cả về số lượng các cuộc tấn công cũng như phương thức, thủ đoạn ngày một tinh vi, gây ra những hậu quả nghiêm trọng hơn, phạm vi và quy mô lớn hơn. Hacker mũ đen/xám tấn công vào bất kỳ chỗ nào có thể, để phá hoại, trộm cắp các thông tin, dữ liệu với đa phần là mục đích xấu. Thời gian qua, nhiều cơ quan Nhà nước của Việt Nam bị tấn công gây hậu quả về tài chính, kinh tế, làm tê liệt công tác quản lý nhà nước và cao hơn ữưa là làm ảnh hưởng ươi uy tín của Việt Nam trên trường quốc tế. Thục tế quá trình làm việc iơsi các cơ quan, đơn vị, Cục C50 nhận thấy: Việc bị hacker tấn công phần lớn là do lỗi chủ quan của cơ quan chủ quản, cụ thể như sau:

-Múc độ quan tâm đến các hệ thống bảo vệ an ninh mạng tại các cơ quan nhà nước và các doanh nghiệp tại Việt Nam là chưa cao. Đây chính là điều kiện thuận lợi cho các đối tượng tội phạm mạng thực hiện các hành vi tấn công, xâm nhập để đánh cắp hoặc phá hoại hệ thống thông tin.

-An ninh, an toàn hệ thống thông tin chưa được coi trọng đúng mức, dẫn đến thiếu sự đầu tư trang thiết bị cũng như nhân lực chất lượng cao.

-Việc sử dụng công nghệ thông tin ở nhiều tổ chức, cá nhân còn thiếu kiến thức cần thiết, vẫn còn tâm lý chủ quan, đơn giản nên dễ tạo ra những "lỗ hổng" dẫn đến lộ, lọt, bị tấn công, mất an toàn thông tin.

-Nhiều đơn vị không có quy chế, quy trình chặt chẽ trong việc bảo mật an toàn hệ thống thông tin dẫn đến tạo lỗ hổng ở ngay chính nhân viên bảo vệ hệ thống.

-Đánh giá múc độ thiệt hại, hậu quả khi xảy ra sự cố hệ thống thông tin ở mức thấp trong khi thực tế có thể xảy ra những hậu quả nghiêm trọng về kinh tế, uy tín, lộ lọt tài liệu mật, ảnh hưởng tiêu cực đến dư luận xã hội...

-Không chuẩn bị sẵn sàng các biện pháp đối phó khi có các rủi ro xảy ra, dẫn đến lúng túng trong xử lý tình huống bị tấn công hoặc bị mất dữ liệu khi bị tấn công.

Chúng tôi đã nhiều lần báo cáo lãnh đạo Bộ Công an về thực trạng trên, trực tiếp xử lý hoặc phối hợp với các cơ quan chức năng như VNCERT, Thanh tra Bộ Thông tin và Truyền thông gửi cảnh báo tới các đơn vị khi phát hiện các nguy cơ có thể xảy ra với an toàn thông tin hệ thống. Điển hình như các vụ việc trộm cắp thông tin khách hàng xảy ra tại VNPT; vụ cổng thông tin điện tử của nhiều địa phương bị chèn mã độc ...Tuy nhiên, nhiều cơ quan, đơn vị chưa quan tâm đúng mức những cảnh báo này.

Để *phòng ngừa bị tin tặc tấn công, các cơ quan chủ quản cần nâng cao năng lực, đảm bảo an toàn, an ninh mạng và chú ý các vấn đề sau:*

-Có tầm nhìn và đầu tư về an ninh mạng tương ứng với quy mô của cơ quan, doanh nghiệp. Đầu tư, nâng cấp hạ tầng kĩ thuật an ninh mạng và triển khai nhiều giải pháp đảm bảo an ninh thông tin. Triển khai các biện pháp quản lý kỹ thuật và quản lý nhân sự. Tùy theo tính chất, nhiệm vụ của cơ quan, đơn vị, cá nhân mà có các hệ thống "tường lửa", thiết bị cảnh báo, phần mềm diệt virus, chống gián điệp... để bảo vệ an toàn thông tin. Thực tế hiện nay các đơn vị còn chủ quan, xem nhẹ vấn đề an ninh, an toàn mạng nên chưa có sự đầu tư cần thiết.

-Thục hiện chính sách an ninh mạng đối với doanh nghiệp, đây là vấn đề cốt lõi để đảm bảo một môi trường mạng an toàn. Các doanh nghiệp, đơn vị trên thế giới đều áp dụng chính sách an ninh hệ thống thông tin theo chuẩn ISO 27001, tiêu chuẩn này quy định chi tiết về phương pháp xây dựng hệ thống thông tin đảm bảo an toàn, các doanh nghiệp cần dựa theo tiêu chuẩn này để áp dụng cho phù hợp với điều kiện của mình.

-Đảm bảo nhân lực an toàn thông tin có trình đô chuyên môn cao, có kinh nghiệm trong phòng ngừa, xử lý các sự cố hệ thống CNTT.

-Nâng cao nhận thức, trách nhiệm của cán bộ, công nhân viên; hiểu đầy đủ và thực hiện đúng các quy định của pháp luật về bảo đảm an toàn thông tin mạng.

-Xây dựng và thực hành các kịch bản phản ứng trong trường hợp hệ thống thông tin bị xảy ra tấn công.

-Thường xuyên tổ chức các chương trình đào tạo, phổ biến, tập huấn để nâng cao nhận thức, kiến thức về an toàn thông tin, tránh bị tin tặc lợi dụng.

Những đơn vị hoạt động trong các lĩnh vực trọng yếu như: Hàng không, điện lực, thủy điện, giao thông, báo chí, ngân hàng, các cơ quan chính phủ... là những lĩnh vực cần chú ý, phòng ngừa cao nhất để tránh những sự cố, rủi ro có thể xảy ra khi hệ *thống thông tin là mục tiêu của tin tặc.*

-Tăng cường kiểm tra, giám sát, phát hiện, xử lý nghiêm các cá nhân, tổ chức vi phạm quy đinh về bảo đảm an toàn thông tin mạng.

Đảm bảo tốt an toàn hệ thống thông tin không chỉ giúp doanh nghiệp tránh được những rủi ro mà còn giúp cho công tác điều tra, xác minh của các cơ quan chúc năng được thuận lợi để ngăn ngừa hệ thống có thể bị lợi dụng, tấn công trở lại.

Nếu phát hiện hệ thống CNTT, các cơ quan chủ quản cần ghi nhận và cung cấp các hiện tượng, dấu hiệu ban đầu cho đơn vị chuyên trách xử lý sự cố an ninh thông tin. Ví dụ: chụp màn hình thể hiện hệ thống bị nhiễm mã độc, thu thập lịch sử truy cập và gửi cho đội ngũ chuyên gia.

Nhanh chóng cách ly hệ thống có dấu hiệu bị tấn công, đồng thời giữ nguyên hiện trường hệ thống đang bị nhiễm, tạm thời sử dụng hệ thống máy chủ dự phòng cho các hệ thống chính.

Tiến hành thay đổi mật khẩu toàn hệ thống, đặc biệt là các hệ thống quan trọng như domain, cơ sở dữ liệu, ứng dụng core...: Backup dữ liệu mới nhất sang các bộ lưu trữ ngoài.

Liên lạc ngay với đơn vị chuyên trách xử lý sự cố an toàn thông tin như VNCERT, Cục C50, Bộ Công an.

1.2. Khái niệm "Chiến tranh thông tin"

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin, sự bùng nổ thông tin là sự hình thành của loại hình chiến tranh mới – Chiến tranh thông tin. Không dùng súng đạn, vũ khí hạt nhân,… để tấn công, Internet sử dụng một công cụ cực kỳ hữu dụng để tấn công đối phương. Các thế lực thù địch lợi dụng sự phát triển của Internet, lợi dụng tự do ngôn luận để tấn công đối phương trên lĩnh vực thông tin, làm sai lệch thông tin, bóp méo sự thật về thông tin của đối phương, thậm trí làm tê liệt các hệ thống thông tin của đối phương. Đặc biệt các thế lực thù địch còn sử dụng các hacker chuyên nghiệp

tập trung tấn công vào cơ sở hạ tầng thông tin của đối phương thuộc các lĩnh vực như: quân sự, tài chính, ngân hàng, mạng máy tính quốc gia,… sử dụng Virus để làm cho hệ thống vũ khí của đối phương bị mất điều khiển, phá hoại cơ sở hạ tầng kinh tế quốc dân làm cho nền kinh tế của đối phương bị rối loạn,… hay đánh cắp những bí mật quân sự, những thông tin quốc gia quan trọng của đối phương.

Trước tình hình đó, các quốc gia trên thế giới đều đang có những bước chuẩn bị để đối phó với chiến tranh thông tin.

Tại Việt Nam, loại hình chiến tranh thông tin ngày càng được hình thành rõ nét. Trong thời gian gần đây, các thế lực thù địch đã lợi dụng mạng Internet để lập các website cá nhân, sử dụng các mạng xã hội đưa những thông tin sai lệch không đúng sự thật về Đảng về Nhà nước lên mạng nhằm bôi xấu, gây mất lòng tin của nhân dân với Đảng và Nhà nước ta. Hàng loạt các website của Việt Nam bị các hacker nước ngoài tấn công làm tê liệt trong một thời gian. Thậm trí có những website Việt Nam bị tấn công còn để lại những hình ảnh và những dòng chữ Trung Quốc [14].

Với xu hướng toàn cầu hoá hiện nay, các mạng lưới truyền thông và xử lý thông tin của các Quốc gia được liên kết với nhau. Do đó ở đâu có điểm kết nối mạng thì ở đó đều có thể xảy ra chiến tranh thông tin. Do vậy các quốc gia cần phải có biện pháp xây dựng các lớp bảo vệ hệ thống thông tin của mình, đồng thời cũng phải chuẩn bị các phương án tấn công các hệ thông tin của đối phương.

Chương 2: CÁC LỖ HỔNG BẢO MẬT MẠNG MÁY TÍNH

2.1. Khái niệm lỗ hổng

Lỗ hổng là các điểm yếu trong phần mềm hoặc phần cứng liên hệ với máy tính cho phép kẻ tấn công phá hoại sự toàn vẹn, độ sẵn sàng hoặc bảo mật của hệ thống. Một số lỗ hổng nguy hiểm nhất cho phép kẻ tấn công khai thác hệ thống bị xâm hại bằng cách khiến hệ thống chạy các mã độc hại mà người dùng không hề biết [7].

Hệ điều hành Microsoft Windows có nguồn gốc phát triển cho các máy tính cá nhân và các mạng an toàn, tuy nhiên nó lại không an toàn đối với mạng phi chính phủ như Internet.

Trong giai đoạn ban đầu, Microsoft thiết kế hệ điều hành Microsoft Windows mà chưa nghĩ tới tầm quan trọng của Internet khi gắn liền với nó. Điều đó đã dẫn tới một số điểm yếu là các lỗ hổng bảo mật(Security holes).

Một lỗ hổng bảo mật cho phép một người nào đó xâm nhập vào máy tính của bạn qua đường kết nối Internet. Những lỗ hổng nhỏ có thể chỉ cho phép truy cập vào clipboard của bạn, nhưng những lỗ hổng lớn có thể cho phép họ tiếp quản hoàn toàn máy tính của bạn.

Các hệ điều hành khác như Linux, Mac OS cũng có các lỗ hổng bảo mật.

Như vậy, lỗ hổng bảo mật là một trong những nguyên nhân dẫn đến sự mất an toàn của các hệ thống máy tính khi kết nối Internet.

Để thực hiện cơ chế an toàn, các hệ điều hành (hoặc các Website) phải được thiết kế để đáp ứng các yêu cầu về mặt an toàn đặt ra. Tuy nhiên, trên thực tế, việc thiết kế các hệ điều hành (hoặc các Website) chỉ đạt đến mức độ tiếp cận các yêu cầu an toàn chứ không đáp ứng được chúng một cách hoàn toàn. Những nơi mà yêu cầu thiết kế bị phá vỡ gọi là các lỗ hổng.

Ví dụ về một số lỗ hổng thường gặp: Lỗi xử lý các yêu cầu không được dự kiến trước trong IIS; lỗi tràn bộ đệm; Điểm yếu trong việc xác thực đối với các tài khoản không mật khẩu hoặc mật khẩu yếu;…

2.2. Các lỗ hổng bảo mật của Hệ Điều Hành.

Lỗ hổng bảo mật trong Knox xuất hiện trên Android

Samsung mới đây cho biết rằng lỗi bảo mật trong tính năng **Knox**được phát hiện hồi tháng trước không chỉ có mặt trên các thiết bị của hãng. Thay vào đó, vấn đề này liên quan đến cả hệ điều hành Android.

Trong một phát ngôn mới đây được đưa ra bởi Samsung và Google, hai công ty nói rằng "*một số chức năng hợp lệ của Android*" có thể bị khai thác theo "*một cách không lường trước*" để can thiệp vào những dữ liệu ứng dụng không mã hóa. Samsung khuyên người dùng nên mã hóa dữ liệu của mình trước khi gửi nó qua Internet bằng những "*công nghệ bảo mật tiêu chuẩn*", ví dụ như VPN (*mạng riêng ảo*) chẳng hạn. Hiện các bên có liên quan đang làm việc để khắc phục vấn đề này.

Phát hiện lỗ hổng bảo mật trên 1.500 ứng dụng iOS

Theo PhoneArena, các nhà nghiên cứu bảo mật đã phát hiện ra một lỗ hổng HTTPS trên 1.500 ứng dụng iOS, cho phép kẻ tấn công khai thác các thông tin cá nhân nhạy cảm của người dùng.

Kaspersky phát hiện lỗi bảo mật trong OS X và iOS

Lỗ hổng này xuất hiện trên phiên bản 2.5.1 của AFNetwork, một thư viện mạng phổ biến của các ứng dụng iOS và Mac OS X. Lỗ hổng được phát hiện từ tháng Hai, bản vá 2.5.2 đã được tung ra vào cuối tháng Ba nhưng vẫn sử dụng phiên bản thư viện cũ nên lỗ hổng vẫn tồn tại.

Trong ngày 1/4, các nhà nghiên cứu của Source DNA đã tiến hành quét **1 triệu** trong số 1,4 triệu ứng dụng trên App Store để tìm kiếm những ứng dụng bị ảnh hưởng bởi lỗ hổng bảo mật trên. Sau khi quét, họ phát hiện ra **1.000 ứng dụng** bị ảnh hưởng, bao gồm cả những ứng dụng từ các hãng công nghệ lớn như Yahoo, Microsoft, Flixster, Citrix và Uber. Ngày 18/4, sau khi quét toàn bộ App Store, các nhà nghiên cứu thống kê được tổng số lượng ứng dụng bị ảnh hưởng là 1.500 ứng dụng [8].

Tin tặc sử dụng lỗ hổng để truy cập vào các liên kết SSL, khai thác các thông tin nhạy cảm như mật khẩu và tài khoản ngân hàng của người dùng.

Độc giả có thể nhấp vào đây để kiểm tra ứng dụng bạn đang sử dụng có bị ảnh hưởng hay không.

Sử dụng tính năng bảo mật mới Smart Lock trên Android 5.0 Lollipop

Phiên bản hệ điều hành mới Android 5.0 Lollipop đi kèm với rất nhiều tính năng mới thú vị. Nhưng một trong những tính năng mới và đáng chú ý nhất chính là Smart Lock vô cùng tiện dụng.

Ý tưởng đằng sau Smart Lock chính là cho phép người dùng dễ dàng bỏ qua mã PIN, mật khẩu hoặc khóa mô hình của màn hình khóa trên điện thoại nếu thiết bị của bạn được kết nối với phụ kiện Bluetooth cụ thể hoặc với một thiết bị hỗ trợ NFC đáng tin cậy.

2.3. Các lỗ hổng bảo mật của mạng máy tính

2.3.1. Các điểm yếu của mạng máy tính

Việc toàn cầu hoá các hoạt động thương mại làm cho sự phụ thuộc tương hỗ ngày càng tăng giữa các hệ thống thông tin. Việc chuẩn hoá công nghệ vì tính hiệu quả và kinh tế song cũng dẫn tới chuẩn hoá tính mỏng manh vốn có của mạng cho kẻ thù lợi dụng, Các quy tắc và tự do hoá cũng đóng góp cho việc tăng thêm tính nguy cơ của an toàn mạng.

Trên thực tế, người ta đã thống kê được 14 lỗ hỏng dễ bị xâm nhập thông qua mạng máy tính. Hình 2-1 minh họa một mô hình mạng tổng quát với các điểm yếu dễ bị xâm nhập, cụ thể:

1.Thiếu điều khiển truy cập bộ định tuyến và lập cấu hình sai ACL sẽ cho phép rò rỉ thông tin thông qua các giao thức ICMP, IP, NetBIOS, dẫn đến truy cập bất hợp pháp các dịch vụ trên máy phục vụ.

2.Điểm truy cập từ xa không được theo dõi và bảo vệ sẽ là phương tiện truy cập dễ dàng nhất đối với mạng công ty.

3.Rò rỉ thông tin có thể cung cấp thông tin phiên bản hệ điều hành và chương trình ứng dụng, người dùng, nhóm, địa chỉ tên miền cho kẻ tấn công thông qua chuyển vùng và các dịch vụ đang chạy như SNMP, finger, SMTP, telnet, rusers, sunrpc, NetBIOS.

4.Máy chủ chạy các dịch vụ không cần thiết (như sunrpc, FTP, DNS, SMTP) sẽ tạo ra lối vào thâm nhập mạng trái phép.

5.Mật mã yếu, dễ đoán, dùng lại ở cấp trạm làm việc có thể dồn máy phục vụ vào chỗ thoả hiệp.

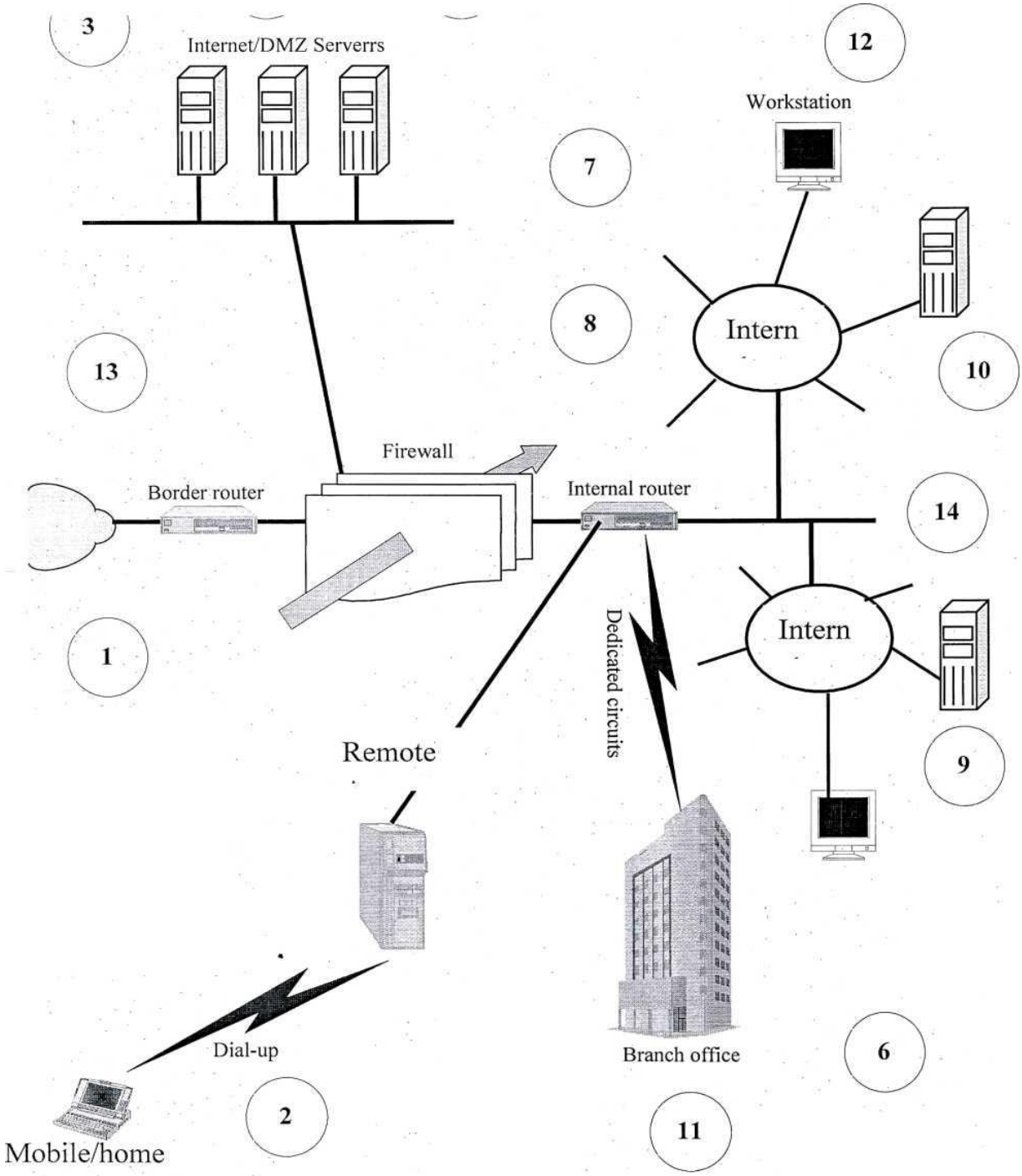
6.Tài khoản người dùng hoặc tài khoản thử nghiệm có đặc quyền quá mức.

7.Máy phục vụ Internet bị lập cấu hình sai, đặc biệt là kịch bản CGI trên máy phục vụ web và FTP nặc danh.

8.Bức tường lửa hoặc ACL bị lập cấu hình sai có thể cho phép truy cập trực tiếp hệ thống trong hoặc một khi đã thoả hiệp xong máy phục vụ.

9.Phần mềm chưa được sửa chữa, lỗi thời, dễ bị tấn công, hoặc để ở cấu hình mặc định.

10.Quá nhiều điều khiển truy cập thư mục và tập tin.



Hình 2-1: Mô hình mạng máy tính

11. Quá nhiều mối quan hệ uỷ quyền như NT domain Trusts, các tập tin .rhosts và hosts.equiv trong UNIX sẽ cho kẻ tấn công truy cập hệ thống bất hợp pháp.

12. Các dịch vụ không chứng thực.

13. Thiếu tính năng ghi nhật ký, theo dõi và dò tại mạng và cấp độ máy chủ.

14. Thiếu chính sách bảo mật, thủ tục và các tiêu chuẩn tối thiểu.

Về phương diện phần mềm:

Các hệ điều hành mạng nổi tiếng mới nhất như Windows 2000, Novel, Linux, Mac os, Unix và các chương trình ứng dụng cũng không tránh khỏi còn tồn tại hàng loạt các lỗ hổng bảo mật giúp cho bọn tin tặc xâm nhập trái phép vào hệ thống mạng và cơ sở dữ liệu của mạng, hiện nay hầu như hàng ngày đều có các thông báo về việc phát hiện ra các lỗ hổng bảo mật trên các hệ điều hành và chương trình ứng dụng ví dụ ngày 6/12/2002 Microsoft đã phát hành một miếng vá mới cho trình duyệt web Internet Explorer. Theo Microsoft, đây là một lỗ hổng có mức độ nguy hiểm "trung bình". Tuy nhiên, các chuyên gia bảo mật máy tính lại coi đây là một lỗ hổng cực kỳ trầm trọng, có thể bị hacker khai thác để nắm quyền điều khiển máy tính. Lỗ hổng ảnh hưởng đến các phiên bản IE 5.5 và IE 6.0. Lỗ hổng này nằm trong cơ chế thiết lập vành đai an ninh giữa cửa sổ trình duyệt web và hệ thống máy tính nội bộ. Việc khai thác lỗ hổng này sẽ cho phép hacker đọc thông tin và chạy các chương trình trong máy tính của người sử dụng. Thậm chí, anh ta còn có thể sửa đổi nội dung một file, format toàn bộ ổ cứng. Nhưng để khai thác được lỗ hổng này, anh ta phải đánh lừa người sử dụng truy cập vào một trang Web đặc biệt do anh ta tạo ra, hoặc mở một e-mail có nhúng mã HTML nguy hại. Ngày 6/10/2002 một công ty chuyên phát triển các chương trình ứng dụng Web của Israel có tên là GreyMagic Software đã phát hiện ra 9 lỗ hổng trong trình duyệt Internet Explorer. Hacker có thể lợi dụng những lỗ hổng này để truy cập vào các file trong máy tính của người sử dụng Internet. GreyMagic Software đánh giá 8 trong số 9 lỗ hổng nói trên có mức độ nguy hiểm cao.

Những lỗ hổng này có thể bị lợi dụng bằng cách như sau: hacker sẽ tạo ra một trang Web chứa các đoạn mã nguy hại, sau đó đánh lừa người sử dụng Internet truy cập vào trang Web này. Khi người sử dụng viếng thăm trang Web, đoạn mã nguy hại sẽ phát huy tác dụng, giúp cho hacker thâm nhập vào máy tính người sử dụng và đánh cắp thông tin. Lee Dagon, Giám đốc nghiên cứu và phát triển của Grey Magic, nói: "Sử dụng những lỗ hổng này kết hợp với một vài lỗ hổng đã biết, hacker có thể dễ dàng xâm nhập vào một máy tính của người sử dụng". Bên cạnh việc cho phép hacker đánh cắp các văn bản trong máy tính, các lỗ hổng còn tạo điều kiện cho hacker sao chép các thông tin, thực thi các chương trình phá hoại và đánh lừa người sử dụng truy cập vào Website nguy hại. GreyMagic cho biết các phiên bản Internet Explorer 5.5 và 6.0 đều tồn tại lỗ hổng, tuy nhiên nếu người sử dụng đã cài bản Internet Explorer 6.0 Service Pack 1 và Internet Explorer 5.5 Service Pack 2 thì sẽ không bị ảnh hưởng...

Theo thống kê của nhóm đề tài các lỗ hổng của hệ điều hành và các chương trình ứng dụng hiện đang sử dụng trên mạng hiện nay là hơn hàng nghìn lỗ hổng, các hãng sản xuất phần mềm liên tục đưa ra các phiên bản để sửa chữa các lỗ hổng đó tuy nhiên hiện nay không ai có thể nói trước được là còn bao nhiêu các lỗ hổng nữa chưa được phát hiện và còn bao nhiêu lỗ hổng đang được sử dụng bí mật bởi các tin tặc và chưa được công bố công khai.

Do cơ chế trao đổi thông tin trên mạng các dich vụ mạng và các lỗ hổng bảo mật hệ thống còn tạo môi trường tốt cho các Virus máy tính phát triển (Virus là một đoạn mã chương trình được gắn kèm vói các chương trình ứng dụng hoặc hệ thống cớ tính năng lây lan rất nhanh và gây nhiều tác hại cho máy tính và dữ liệu).

Theo Chuyên gia Eugene Kaspersky, người đứng đầu nhóm nghiên cứu virus của Kaspersky Labs thì bất cứ hệ thống nào cũng đều phải tuân theo 3

quy luật một khi muốn nhiễm virus. Trước hết, nó phải có khả năng chạy những ứng dụng khác, có nghĩa là bắt buộc phải là một hệ điều hành. Microsoft Office là một hệ điều hành như thế bởi vì nó có thể chạy các macro. Vì thế, khi chúng ta nói về hệ điều hành cho virus, chúng ta không chỉ đề cập đến Windows hay Linux, mà đôi khi cả về những ứng dụng như Microsoft Office... Hơn nữa, hệ điều hành này phải có độ phổ biến cao bởi vì một loại virus muốn phát triển được thì cần phải có người viết ra nó, và nếu như không có tác giả nào sử dụng hệ điều hành, khi đó sẽ không có virus nữa. Thứ hai, hệ điều hành cần phải có đầy đủ tư liệu, nếu không sẽ không thể viết ra một loại virus nào cả. Hãy so sánh máy chủ Linux và Novell: Linux cung cấp đầy đủ tư liệu còn Novell thì không. Kết quả là trong khi có khoảng 100 loại virus trong Linux, chỉ có duy nhất một virus Trojan chuyên gài bẫy mật khẩu trong Novell mà thôi. Cuối cùng, hệ điều hành này phải không được bảo vệ, hoặc là có những lỗ hổng bảo mật. Trong trường hợp của Java, hệ điều hành này có khoảng 3 loại virus, nhưng chúng cũng không thể nhân bản nếu không có sự cho phép của người sử dụng, do đó, Java tương đối miễn nhiễm với virus.

Nói tóm lại, để bị nhiễm virus, một hệ thống cần phải thoả mãn ba điều kiện: phổ biến, đầy đủ tài liệu và sơ hở trong bảo vệ.

Bảng dưới đây minh hoạ các khả năng tin tặc tấn công vào hệ thống mạng máy tính qua các điểm yếu của mạng, các lỗ hổng mạng và yếu tố của con người

Dựa vào yếu tố con người - các điểm yếu của người sử dụng

- Thông tin có sẵn tự do
- Lựa chọn mật khẩu quá đơn giản
- Cấu hình hệ thống đơn giản
- Tính mỏng manh đối với "nền kỹ nghệ đã mang tính xã hội" .

Dựa vào khe hở xác thực

- Trộm mật khẩu
- Nền kỹ nghệ đã mang tính xã hội
- Qua hệ thống mật nhưng bị sụp đổ.

Dựa vào dữ liệu

- Gắn E-mail vào một chương trình
- Các ngôn ngữ lập trình nhúng
    - □ Các lệnh macro của Microsoft word
    - □ Máy in PostScript
- Phần mềm xâm nhập từ xa

  JAVA, Active-X

Dựa trên phần mềm điều khiển và ứng dụng

- Viruses
- Lỗ thủng an ninh
- Các đặc quyền
- Các đặc tính an ninh không sử dụng
- Cửa sau
- Cấu hình hệ thống nghèo nàn. .

Dựa trên giao thức trao đổi thông tin

- Xác thực yếu
- Dãy số dễ đoán
- Nguồn định tuyến cho các gói dữ liệu
- Các trường header không sử dụng .

Từ chối dịch vụ

- Làm tràn ngập mạng
- "Băm nát"
- Sâu Morris.

Yếu kém của hệ thống mật mã

- Các đặc tính/kích cỡ khoá không phù hợp
- Các lỗ hổng thuật toán.

Quản lý khoá

- Suy đoán khoá
- Thay khoá
- Chặn khoá
- Đặt khoá.

Chặn bắt truyền thông trên mạng

- Bắt dữ liệu trước khi mã hoá và thu dữ liệu sau khi giải mã.
- Loại bỏ mã hoá
- Phát lại.

2.3.2. Hiểm hoạ chiến tranh thông tin trên mạng

Mục tiêu của việc kết nối mạng là để nhiều người sử dụng từ những vị trí địa lý khác nhau, có thể dùng chung những tài nguyên, đặc biệt là tài nguyên thông tin. Do đặc điểm của nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên đó tránh khỏi sự mất mát, xâm phạm (vô tình hay hữu ý) phức tạp hơn rất nhiều so với trường hợp máy tính đơn lẻ, một người sử dụng.

Để việc đảm bảo thông tin đạt kết quả cao, chúng ta phải lường trước được càng nhiều càng tốt các khả năng xâm phạm, các sự cố rủi ro đối với thiết bị và tài nguyên trên mạng.

Xác định càng chính xác các nguy cơ trên, ta càng quyết định được tốt các giải pháp phù hợp để giảm thiểu các thiệt hại.

An toàn thông tin là một quá trình tiến triển hợp logic: khi những vui thích ban đầu về một xa lộ thông tin, bạn nhất định nhận thấy rằng không chỉ cho phép bạn truy cập vào nhiều nơi trên thế giới, Internet còn cho phép nhiều

người không mời mà tự ý ghé thăm máy tính của bạn, Internet có những kỹ thuật tuyệt vời cho phép mọi người truy cập, khai thác, chia sẻ thông tin. Nhưng nó cũng là nguy cơ chính dẫn đến thông tin của bạn bị hư hỏng hoặc bị phá huỷ hoàn toàn.

Mục tiêu của chiến tranh chống lại các xã hội dựa trên nông nghiệp là giành quyền kiểm soát nguồn của cải chính của chúng: đó là ruộng đất. Các chiến dịch quân sự được tổ chức để huỷ diệt khả năng của kẻ thù bảo vệ các vùng đất đai. Mục tiêu của chiến tranh chống lại các xã hội dựa trên công nghiệp là giành quyền kiểm soát nguồn tạo ra mọi của cải chính của nó là: các phương tiện sản xuất. Các chiến dịch quân sự được tổ chức để huỷ diệt khả năng cửa kẻ thù giữ quyền kiểm soát các nguồn lực nguyên vật liệu, khả năng sản xuất và lao động.

Mục tiêu của chiến tranh chống lại các xã hội dựa trên thông tin là giành quyền kiểm soát các phương tiện chính nuôi dưỡng và tạo ra mọi của cải: khả năng phối hợp các sự phụ thuộc lẫn nhau về kinh tế - xã hội. Các chiến dịch quân sự được tổ chức để huỷ diệt khả năng của một xã hội dựa trên thông tin vận hành cỗ máy phụ thuộc thông tin của nó.

Xu hướng khai thác tối đa tài nguyên mạng máy tính toàn cầu nhằm phục vụ cho lợi ích cộng đồng là xu hướng tất yếu và cũng chính từ nguồn tài nguyên này, từ môi trường này đã bắt đầu một khái niệm chiến tranh mới: *chiến tranh thông tin trên mạng.*

Cho đến nay chưa có một tài liệu công khai nào đưa ra khái niệm *chiến tranh thông tin* (CTTT) mặc dù cuộc chiến đó đã, đang và tiếp tục diễn ra với mức độ tinh vi cũng như hậu quả do nó gây ra ngày càng cao. Tuy vậy, có thể hiểu: **chiến tranh thông tin là các hành động tiến hành để đạt được ưu thế về thông tin nhằm đánh bại đối phương, bằng cách tác động tới:**

. Thông tin,

. Các quả trình dựa trên thông tin,

. Các hệ thông thông tin của chúng;

trong khi bảo vệ các đối tượng đó của mình.

Đặc điểm của chiến tranh thông tin:

- Trong khi ảnh hưởng và hậu quả của CTTT có thể rất lớn thì vũ khí và phương tiện

  CTTT lại rất rẻ

Điều này là có thể vì thông tin và hệ thống thông tin (đối tượng của cuộc tấn công CTTT) "Một ngôi nhà mà giá trị của nó rẻ hơn cái tàng trữ trong đó", nhiều khi chỉ là một phần tử khiêm tốn lại quyết định một chức năng hoặc một hoạt động quan trọng - như một cơ sở dữ liệu chẳng hạn. Chỉ cần một chi phí thấp để tạo ra một nội gián, một thông tin giả, thay đổi thông tin, hoặc đưa ra một vũ khí logic tinh vi chống lại một hệ thống thông tin được nối vào hạ tầng viễn thông dùng chung toàn cầu. vấn đề cuối này lại càng hấp dẫn; những thông tin mới nhất về cách thức khai thác các đặc tính thiết kế và lỗ hổng an ninh của các phần mềm máy tính thương mại đang tự do lưu truyền trên Internet.

- Về phía tấn công, CTTT rất hấp dẫn

Chiến tranh thông tin tấn công rất hấp dẫn đối với nhiều người vì nó rẻ so với chi phí phát triển, duy trì, và dùng các khả năng quân sự tiên tiến. Thêm vào đó, kẻ tấn công có thể bị lôi cuốn vào CTTT bởi tiềm năng đối với các kết quả đầu ra không tuyến tính khổng lồ lấy từ các đầu vào khiêm tốn.

Rất nhiều người bình thường chỉ cần với một máy tính kết nối mạng đều có khả năng thử sức khai phá cả thế giới tài nguyên hấp dẫn trên mạng, nhiều công cụ họ tạo ra ban đầu chỉ là thử sức và để đùa cho vui và chứng tỏ

tài năng vói mọi người xung quanh sau đã bị các kẻ phá hoại lợi dụng biến thành các vũ khi tấn công trên mạng.

- Về phía phòng thủ, CTTT chứa nhiều yếu tố bất ngờ và khó tiên liệu trước

CTTT là một khái niệm rộng lớn, biến đổi theo thời gian và không gian. Cách phòng chống và đánh trả CTTT cũng hết sức linh hoạt vì nó liên quan đến nhiều lĩnh vực như *các tiêu chuẩn an toàn của hệ thống, cơ sở pháp lý về an ninh mạng của mỗi quốc gia, khả năng cũng như trình độ của con người... và sau cùng là các kỹ thuật-công nghệ* được áp dụng vào cuộc chiến tranh này.

Thực tiễn làm nẩy sinh các cuộc tấn công bao gồm các ứng dụng phần mềm được thiết kế tồi; việc sử dụng các hệ điều hành phức tạp nhưng kém bảo mật nội tại; sự thiếu huấn luyện và thiếu các công cụ giám sát và quản lý môi trường tính toán từ xa; sự nối mạng cẩu thả các máy tính tạo ra tiềm năng gây lỗi; sự huấn luyện chưa phù hợp các nhân viên quản trị thông tin; và sự thiếu thốn các quy trình mạnh để nhận dạng các phần tử hệ thống, kể cả nhận dạng người sử dụng. Quan trọng nhất vẫn là việc dựa các chức năng quân sự, kinh tế và xã hội vào các hệ thống được thiết kế tồi, và bố trí cho các hệ thống này các lực lượng chuyên môn không đủ kinh nghiệm. Các nhân viên này thường ít chú ý tới hoặc không hiếu biết về hệ quả của các hỏng hóc hệ thống thông tin, sự mất mát tính toàn vẹn dữ liệu, hoặc mất tính bảo mật dữ liệu. Chi phí cho phòng thủ trong CTTT không rẻ, cũng không dễ dàng thiết lập. Nó sẽ cần các nguồn lực để phát triển các công cụ, quy trình, và các thủ tục để đảm bảo tính sẵn sàng và toàn vẹn của thông tin, và để bảo vệ tính bảo mật thông tin ở nơi cần đến nó. Các nguồn lực bổ sung sẽ cần để phát triển các hướng dẫn thiết kế cho các kỹ sư hệ thống và phần mềm để đảm bảo các hệ thống thông tin có thể hoạt động trong một môi trường CTTT. Nhiều nguồn lực hơn sẽ cần để phát triển các phương tiện mạnh nhằm phát hiện kẻ nội gián

đột nhập với ác ý can thiệp vào các hệ thống và để chúng ta có khả năng tiến hành sửa đổi và khôi phục hệ thống.

- Càng phát triển theo hướng một xã hội thông tin thì hiểm hoạ CTTT lại càng lớn, và do đó - CTTT là không thể tránh khỏi.

Trong xu thế xã hội hoá mạng thông tin, dù ngăn chặn thế nào thì những cuộc tấn công trên mạng vẫn khó tránh khỏi bởi con người luôn lệ thuộc vào thông tin còn kẻ tấn cống (hacker) luôn hứng thú với sức mạnh ảo mà các cuộc tấn công mang lại.

Nhiều quan điểm về tương lai của an ninh mạng được đưa ra, ví dụ như một số chuyên gia an ninh mạng của Mỹ dự báo: "Với hơn 100 triệu máy vi tính liên kết chặt chẽ chúng ta lại với nhau thông qua một loạt các hệ thống liên lạc ở mặt đất và trên vệ tinh... Ngày nay các hệ thống vi tính của chính phủ và của ngành thương mại được bảo vệ quá sơ sài đến mức có thể coi là không được bảo vệ gì. Một trận "Trân Châu Cảng" điện tử đang sắp sửa xảy ra".

Chúng ta không thể coi nhẹ các phương pháp tấn công của các hacker. Nhiều trong số các phương pháp này là đủ mạnh để phá hoại hoặc tấn công khủng bố trên quy mô lớn. Các phân mềm ác ý có thể được triển khai trước với các việc kích hoạt tuỳ theo thời điểm hoặc bằng các phương tiện kích hoạt khác và rằng hiệu quả có thể là một cuộc tấn công đồng thời trên diện rộng. Một cuộc tấn công như vậy không thể coi là không có, mặc dù xác suất của nó được đánh giá là thấp.

Về nguyên tắc, các hình thức tiến hành chiến tranh thông tin đã sử dụng và được nêu ra là hiểm hoạ có thật. Những kỹ thuật cơ bản để phòng tránh các hình thức chiến tranh này vẫn đang được các nước chú trọng nghiên cứu.

Sự đe doạ với một hệ thống mở

Một hệ thống mở là một hệ thống cho phép tính tương tác mềm dẻo, các phần mềm và thành phần của hệ thống có thể thêm bớt tuỳ ý. Trước khi có sự tiếp cận theo hệ thống mở, nhiều nhà sản xuất cho rằng tốt hơn cần bảo vệ tính riêng tư. Hệ điều hành UNIX là một trong những ví dụ điển hình cho việc hướng tới một hệ thống mở.

Ngày nay, nói đến sự phát triển của Internet không thể không nói đến hệ thống mở. Với sự ra đời của bộ giao thức *TCP/IP*, và sự phát triển của World Wide Web (WWW) hệ thống mở càng chứng tỏ khả năng ưu việt của mình. Nhưng bên cạnh đó, một vấn đề mới lại nảy sinh, an toàn bảo mật trong hệ thống mở. Với sự phát triển của Internet, không còn mạng máy tính nào là biệt lập. Từ bất kỳ đâu, chỉ với một chiếc máy tính nối với Internet, bất kỳ ai đều có thể xâm nhập vào một mạng máy tính nào đó có kết nối Internet. Với khả năng truy cập lớn như vậy, tính bảo mật là một vấn đề nghiêm chỉnh cần được xem xét. Vì thế, *Firewall* được coi là giải pháp không thể thiếu khi cần kiểm soát sự truy cập tại một mạng máy tính dù là cục bộ hay diện rộng. Với những ưu việt của mô hình hệ thống mở, những trở ngại về an ninh cũng ngày càng tăng. Tính bảo mật và sự truy cập tới mạng là hai đại lượng luôn tỉ lệ nghịch với nhau. Tính mở luôn là một con dao hai lưỡi. Nó mang lại sự kết nối thật dễ dàng nhưng cũng làm tăng các kẽ hở cho những ai tò mò.

2.4. Một số lỗ hổng do người dùng vô tình gây ra.

Lỗ hổng kiến thức về an ninh mạng ở Việt Nam khiến người dùng có thể gặp nguy hiểm

Ngày 7/12/2015, ESET, nhà tiên phong về phòng vệ chủ động đã công bố Báo cáo của ESET về Nhận thức An ninh mạng tại Việt năm 2015. Báo cáo chỉ ra rằng người dùng tại Việt Nam có nhận thức thấp về an ninh mạng và chưa có các biện pháp phòng ngừa thích hợp, khiến họ dễ bị các mối nguy cơ trực tuyến đe dọa. Kết quả khảo sát cho thấy trong khi 87% người dùng

trên cả nước lo lắng về các nguy cơ trực tuyến, chỉ 32% có các biện pháp bảo vệ đúng đắn trước các mối nguy hiểm này - đây là tỷ lệ thấp nhất trong khu vực châu Á - Thái Bình Dương [2].

Cuộc khảo sát thăm dò ý kiến của 500 người tại Việt được thực hiện nhằm tìm hiểu rõ thái độ, kiến thức và hành vi của người dùng về an ninh mạng. Kết quả kháo sát được công bố tại Hội nghị Quốc tế về Phòng chống Mã độc Toàn cầu 2015 lần thứ 18 diễn ra tại Đà Nẵng, Việt Nam.

Khi so sánh với kết quả trong Báo cáo của ESET về Nhận thức An ninh mạng khu vực châu Á năm 2015 được thực hiện tại 6 thị trường khác trong khu vực châu Á - Thái Bình Dương, Việt Nam đứng cuối về nhận thức về an ninh mạng, sau Malaysia, Singapore, Ấn Độ, Thái Lan, Hồng Kông và Indonesia (xếp theo thứ tự từ cao đến thấp). Mức độ nhận thức về an ninh mạng được đánh giá dựa trên các yếu tố như: kiến thức hoặc khả năng hiểu biết các hoạt động có thể gây nguy cơ cho người dùng, các hành vi nguy hiểm khi lướt web, và các biện pháp chủ động trước các mối nguy hiểm này.

"Do sự bùng nổ mạnh mẽ của Internet, Việt Nam đang ngày càng phụ thuộc nhiều hơn vào dữ liệu, giao tiếp điện tử và công nghệ thông tin để cải tiến và nâng cao hiệu suất, hệ quả là các nguy cơ về an ninh mạng ngày một gia tăng," ông Parvinder Wali, Giám đốc Bán hàng và Marketing, Tập đoàn ESET khu vực châu Á - Thái Bình Dương chia sẻ. "Báo cáo của ESET về Nhận thức An ninh mạng tại Việt Nam năm 2015 nhấn mạnh rằng mặc dù người dùng Internet tại Việt Nam biết một số hành động nào đó có thể khiến họ gặp rủi ro hoặc dễ bị tấn công khi trực tuyến, nhưng họ vẫn không ngừng mắc sai lầm. Khe hở giữa nhận thức và hành động này là một xu hướng đáng lo ngại vì tin tặc thường tấn công những chỗ ít đề phòng nhất. Nếu người dùng không có đủ các biện pháp phòng ngừa thích hợp, họ có thể vô tình trở thành nạn nhận của một cuộc tấn công mạng".

Kết quả chính của cuộc khảo sát cho thấy đa số những người sử dụng Internet ở Việt có quan niệm sai lầm về những vấn đề an ninh mạng phổ biến. Nhiều người không thể trả lời đúng những câu hỏi như sự nguy hiểm của việc sử dụng wifi công cộng miễn phí (59% cho rằng việc này an toàn) cũng như của việc tạo mã bảo mật với các thông tin cá nhân (70% nghĩ rằng việc này an toàn). 62% người dùng cũng tin vào "huyền thoại" rằng máy tính để bàn dễ bị hack hơn các thiết bị di động. Con số này càng nhấn mạnh sự thiếu nhận thức về an ninh mạng tại Việt .

Người dùng Việt lo ngại nhất về sự an toàn của các thông tin nhạy cảm trên các thiết bị cá nhân của mình và việc bảo vệ các thiết bị này khỏi vi-rút. Đáng lo ngại là chỉ có khoảng 30% người được hỏi nhận thức được những rủi ro nghiêm trọng do các mối đe dọa chung gây ra như các ứng dụng không có đảm bảo, thư rác và các quảng cáo banner, điều này một lần nữa cho thấy rằng lỗ hổng kiến thức có thể khiến người dùng dễ dàng bị tấn công.

Các hành vi trực tuyến gây nguy hiểm đang phổ biến rộng rãi

Người dùng tại Việt Nam gặp phải những sai lầm cơ bản như kết nối wifi công cộng không đảm bảo (71%), tạo mật mã dễ nhớ (70%), không thay đổi mật mã trong thời gian dài (66%), cài đặt đăng nhập tài khoản tự động (59%), và tải các tập tin từ các nguồn không chính thức (49%). Kết quả khảo sát cho thấy, trung bình, hơn 68% những người trong độ tuổi từ 18-24 tại Việt Nam có những hành vi trực tuyến gây nguy hiểm.

Ông Walia cho biết thêm: "Điều quan trọng là chúng ta cần phải tăng cường nhận thức về an ninh mạng và xóa bỏ các "huyền thoại" về vấn đề này. Người dùng Internet ở Việt Nam vẫn gặp phải những rủi ro không đáng có khi online, một phần do sự thiếu hiểu biết và một phần do quan niệm sai lầm rằng các tài khoản cá nhân và các hoạt động trực tuyến không phải là mục tiêu của tin tặc. Thật đáng tiếc vì chỉ cần áp dụng những bước đơn giản, như thường

xuyên thay đổi mật khẩu, cũng làm giảm đáng kể nguy cơ bị hack, khiến người dùng an toàn và tự tin hơn khi lướt web".

2.5. Hackers và hậu quả mà chúng gây ra

2.5.1. Hacker

Quản Trị Mạng - Nhờ các phương tiện truyền thông, từ " hacker" đã được biết đến với tiếng xấu. Khi nói tới từ này, mọi người đều nghĩ đến những kẻ xấu có kiến thức về máy tính luôn tìm cách để hại mọi người, lừa gạt các tập đoàn, ăn cắp thông tin và thậm chí là phá hoại nền kinh tế hoặc gây ra chiến tranh bằng cách thâm nhập vào hệ thống máy tính quân đội. Mặc dù chúng ta không thể phủ nhận vẫn còn một số hacker không có mục đích xấu, họ vẫn chỉ chiếm phần nhỏ trong cộng đồng hacker.

Thuật ngữ "hacker" máy tính lần đầu tiên được sử dụng vào giữa những năm 1960. Một hacker vốn là một lập trình viên – kẻ đã hack code máy tính. Hacker có khả năng tìm kiếm nhiều cách khác nhau để sử dụng máy tính, tạo các chương trình mà không ai có thể hiểu được. Chúng là những người tiên phong đi đầu trong ngành công nghiệp máy tính khi xây dựng mọi thứ từ những ứng dụng nhỏ dành cho hệ điều hành. Trong lĩnh vực này, những người như Bill Gates, Steve Jobs và Steve Wozniak đều là hacker khi họ có thể nhận biết được khả năng máy tính có thể làm được gì và tạo ra các cách khác nhau để đạt được những khả năng đó.

Một cách gọi thống nhất dành cho những hacker trên là sự ham hiểu biết, ham học hỏi. Những hacker này tự hào không chỉ về khả năng tạo chương trình mới, mà còn về khả năng biết cách những chương trình khác cùng với hệ thống hoạt động như thế nào. Mỗi khi một chương trình có một

bug – lỗi kỹ thuật khiến chương trình khó có thể hoạt động – hacker thường tạo ra một bản patch – bản vá để chữa lỗi. Một số người đã chọn nghề có thể nâng cao kỹ năng của họ, nhận tiền từ những phần mềm họ tạo ra.

Cùng với sự phát triển của máy tính, các nhà lập trình viên máy tính bắt đầu kết nối với nhau thành một hệ thống. Không lâu sau đó, thuật ngữ hacker đã có nghĩa mới – những kẻ sử dụng máy tính để đột nhập vào một mạng lưới mà họ không phải là thành viên. Thông thường, hacker không có ý đồ xấu. Họ chỉ muốn biết được máy tính trong một mạng làm việc như thế nào và liệu có một rào cản nào đó giữa chúng.

Thực tế, điều này vẫn xảy ra ngày nay. Trong khi có rất nhiều câu chuyện về các hacker xấu phá hoại hệ thống máy tính, xâm nhập vào mạng và phát tán virus. Hầu hết các hacker rất tò mò, họ muốn biết tất cả những sự phức tạp của thế giới máy tính. Một số sử dụng kiến thức của mình để giúp các tổ chức và chính phủ xây dựng một hệ thống bảo mật an toàn hơn. Một số khác có thể sử dụng kỹ năng của mình vào mục đích xấu. Ngày nay, hackers có thể là một tổ chức được Một Nhà nước hỗ trợ tối đa nhằm đánh cắp hoặc phá hủy Hệ thống thông tin đối phương. Do đó chúng cực kỳ nguy hiểm đối với không những các cá nhận, Doanh nghiệp, mà còn đối với sự tồn vong của cả Quốc gia.

Trong phạm vị của Luận văn này, chúng ta chỉ tìm hiểu những kỹ năng thông thường hacker hay sử dụng để thâm nhập hệ thống máy tính, khám phá về văn hóa hacker cùng với các loại hacker khác nhau. Ngoài ra, Luận văn cũng còn nói về một vài hacker nổi tiếng.

Hệ thống cấp bậc hacker

Theo nhà tâm lý học Marc Rogers, có một số nhóm nhỏ của hacker như newbies, cyberpunks, coders và cyber terrorists. Newbies là những kẻ truy cập trái phép mà không nhận thức được máy tính và các chương trình hoạt

động như thế nào. Cyberpunk là những kẻ có hiểu biết và khó bị phát hiện và bị bắt hơn so với newbie khi xâm nhập hệ thống, bởi chúng có xu hướng khoe khoang về sự hiểu biết. Coder viết các chương trình để các hacker khác sử dụng vào việc xâm nhập hệ thống và điều khiển hệ thống máy tính. Một cyber terrorist là hacker chuyện nghiệp chuyên xâm nhập hệ thống để kiếm lợi nhuận. Chúng có thể phá hoại cơ sở dữ liệu của một công ty hay một tập đoàn để sở hữu những thông tin quan trọng.

Đối với những hacker trên, ngoài tài năng và sự hiểu biết là code. Trong khi có một cộng đồng hacker lớn trên mạng Internet, chỉ có một số nhỏ trong chúng thực sự có khả năng code chương trình. Rất nhiều hacker tìm kiếm và tải code được viết bởi người khác. Có rất nhiều chương trình khác nhau mà hacker sử dụng để thâm nhập vào máy tính và mạng. Những chương trình này giúp hacker rất nhiều, một khi chúng biết cách hoạt động của một hệ thống, chúng có thể tạo ra các chương trình để khai thác hệ thống đó.

Những hacker nguy hiểm thường sử dụng các chương trình để :

.Khóa bàn phím:

Một số chương trình giúp các hacker nhận tất cả những gì người dùng máy tính gõ vào bàn phím. Sau khi đã được cài đặt trên máy của nạn nhân, chương trình sẽ ghi lại toàn bộ các phím trên bàn mà người dùng gõ, cung cấp mọi thông tin để hacker có thể xâm nhập vào hệ thống, thậm chí là ăn cắp thông tin cá nhân quan trọng của người dùng.

• **Hack mật khẩu**: Có rất nhiều cách để ăn trộm mật khẩu của ai đó, từ việc đoán mật khẩu cho tới việc tạo ra các thuật toán để kết hợp các kí tự, con số và biểu tượng. Họ cũng có thể sử dụng cách tấn công brute force, có nghĩa là hacker sử dụng tất cả các kiểu kết hợp khác nhau để có thể truy cập. Một cách khác là phá mật khẩu bằng cách sử dụng kiểu tấn công từ điển

(dictionary attack), một chương trình có khả năng điền những từ thông thường vào mật khẩu.

• **Lây nhiễm một máy tính hoặc một hệ thống với virus:** Virus máy tính là những chương trình được thiết kế để tự sao chép và gây các lỗi như xâm nhập vào máy tính để xóa sạch mọi thứ trong ổ đĩa hệ thống. Hacker có thể tạo ra một virus để xâm nhập hệ thống, nhưng nhiều hacker khác thường tạo một virus rồi gửi chúng tới những nạn nhân tiềm năng thông qua email, tin nhắn nhanh hay các website với nội dung có thể tải được hoặc qua các mạng đồng đẳng.

• **Gain backdoor access:** Giống với hack mật khẩu, một số hacker tạo các chương trình để tìm kiếm những đường dẫn không được bảo vệ để thâm nhập vào máy tính và hệ thống mạng. Trong thời gian đầu của Internet, rất nhiều hệ thống máy tính không có nhiều biện pháp bảo vệ, tạo điều kiện cho hacker tìm kiếm đường dẫn vào hệ thống mà không cần tới tài khoản và mật khẩu. Một cách khác hacker hay sử dụng để lây nhiễm một máy tính hoặc một mạng là sử dụng Trojan horse. Không giống như virus, trojan không có chức năng tự sao chép nhưng lại có chức năng hủy hoại tương tự virus. Một trong những thứ giăng bẫy của Trojan horse là nó tự nhận là giúp cho máy của thân chủ chống lại virus nhưng thay vì làm vậy nó quay ra đem virus vào máy.

• **Tạo một máy tính ảo:** Một máy tính ảo là máy tính hacker dùng để gửi spam hoặc thực hiện kiểu tấn công Distributed Denial of Service (DDoS – tấn công từ chối dịch vụ phân tán). Sau khi nạn nhân chạy một đoạn code, kết nối được mở ra giữa máy tính của nạn nhân với hệ thống của hacker. Hacker có thể bí mật kiểm soát máy tính của nạn nhân, sử dụng nó để thực hiện mục đích xấu hoặc phát tán spam.

• **Gián điệp trên email:** Hacker đã tạo code để giúp chúng chặn và đọc email, một cách gần giống như nghe trộm. Ngày nay, hầu hết các email đều

được mã hóa phức tạp để phòng trừ trường hợp nếu emai này bị hacker chặn, hắn cũng không thể đọc được nội dung bên trong.

Văn hóa Hacker

Phreak siêu đẳng

Trước khi có hacker máy tính, những kẻ thông minh nhưng rất hay tò mò đã tìm các cách khác nhau để thâm nhập vào hệ thống điện thoại, được gọi là phreaking. Bằng cách phreaking, những người này có thể thực hiện một cuộc gọi dài miễn phí hoặc thậm chí là thực hiện cuộc gọi trên máy của người khác.

Rất nhiều hacker là những kẻ khó gần gũi. Sở thích mãnh liệt nhất của chúng là máy tính và lập trình có thể trở thành rào cản giao tiếp. Để chúng với các thiết bị riêng, một hacker có thể bỏ ra hàng giờ làm việc trên máy tính và quên đi mọi thứ xung quanh.

Mạng Internet đã tạo cơ hội cho hacker có thể gặp những người cùng sở thích. Trước khi Internet trở nên dễ dàng tiếp cận, hacker đã có thể thiết lập và truy cập bulletin board systems (BBS - Hệ thống bảng tin trên nền máy tính). Một hacker có thể "đăng cai" một BBS trên máy tính của họ rồi cho phép mọi người truy cập vào hệ thống để gửi tin nhắn, chia sẻ thông tin, chơi game và tải các chương trình. Hacker này chia sẻ thông tin cho hacker khác, thông tin được chia sẻ một cách nhanh chóng.

Một số hacker còn đăng tải thành tích của mình trên BBS, khoe khoang về việc đã thâm nhập một hệ thống bảo mật. Thông thường, chúng sẽ đăng tải một tài liệu nào đó từ cơ sở dữ liệu của nạn nhân để chứng minh. Vào đầu những năm 1990, cơ quan hành pháp chính thức coi các hacker là mối đe dọa lớn đối với hệ thống bảo mật. Có hàng trăm người có thể hack hệ thống bảo mật nhất trên thế giới.

Ngoài ra, có rất nhiều trang Web được tạo ra dành cho hack. Thời báo "*2600: The Hacker Quarterly*" [.] đã dành riêng các chuyện mục dành cho hacker. Các bản được in ra vẫn có trên các quầy báo. Các trang khác như Hacker.org còn tích cực ủng hộ việc học, trả lời các câu đố hay tổ chức các cuộc thi dành cho hacker để kiểm tra kỹ năng của chúng.

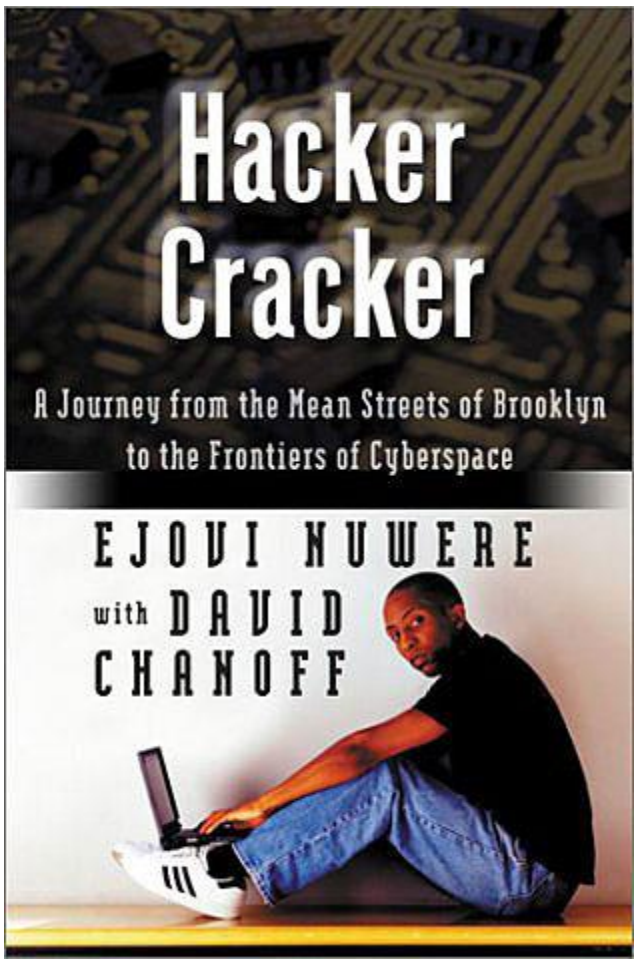
Khi bị bắt bởi cơ quan hành pháp hoặc các tập đoàn, một số hacker thừa nhận rằng họ có thể gây ra vấn đề lớn. Hầu hết các hacker đều không muốn gặp rắc rối, thay vào đó, họ hack hệ thống chỉ bởi muốn biết hệ thống đó hoạt động như thế nào. Đối với một hacker, hệ thống bảo mật như Mt. Everest, chúng xâm nhập chỉ vì thử thách tuyệt đối. Tại Mỹ, một hacker có thể gặp rắc rối khi chỉ đơn giản là đi vào một hệ thống. Điều luật về lạm dụng và gian lận máy tính không cho phép truy cập hệ thống máy tính.

Hacker và Cracker

Rất nhiều lập trình viên khăng khăng cho rằng từ hacker được áp dụng cho những người tôn trọng luật pháp, những người tạo ra các chương trình và ứng dung hoặc tăng khả năng bảo mật cho máy tính. Còn đối với bất kì ai sử dụng kỹ năng với ý đồ xấu đều không phải là hacker mà là cracker.

Cracker xâm nhập hệ thống và gây thiệt hại hoặc tệ hơn thế. Không may rằng, hầu hết mọi người không thuộc cộng đồng hacker đều sử dụng từ hacker như một nghĩa xấu bởi họ không biết cách phân biệt giữa hacker và cracker.

Không phải tất cả hacker đều muốn truy cập những hệ thống máy tính. Một số người sử dụng kiến thức và sự thông minh của mình để tạo ra những phần mềm tốt, các biện pháp bảo mật an toàn. Thực tế, rất nhiều hacker đã từng đột nhập vào hệ thống, sau đó đã sử dụng sự hiểu biết, sự khéo léo của mình để tạo ra những phương pháp bảo mật an toàn hơn. Nói theo cách khác, Internet là sân chơi giữa những kiểu hacker khác nhau – những kẻ xấu, hoặc mũ đen, những người luôn tìm mọi cách để xâm nhập trái phép hệ thống hoặc phát tán virut và những người tốt, hoặc mũ trắng, những người luôn tăng cường cho hệ thống bảo mật và phát triển những phần mềm diệt virut "khủng".



Tuy vậy, hacker, theo cả 2 bên đều hỗ trợ các phần mềm mã nguồn mở, chương trình mà nguồn code có sẵn cho mọi người học, sao chép, chỉnh sửa. Với các phần mềm mã nguồn mở, hacker có thể học từ kinh nghiệm của các hacker khác và và giúp tạo ra các chương trình hoạt động tốt hơn trước đây. Các chương trình có thể là những ứng dụng đơn giản tới hệ điều hành phức tạp như Linux.

Có một số sự kiện về hacker hàng năm, hầu hết là ủng hộ các hành động chịu trách nhiệm. Một hội nghị được tổ chức hàng năm ở Las Vegas có tên DEFCON thu hút được hàng ngàn người tham gia để trao đổi các phần mềm, tham dự các cuộc tranh luận, hội thảo về hack và phát triển máy tính cũng như thỏa mãn sự tò mò của mình. Một sự kiện tương tự có tên Chaos Communication Camp để chia sẻ phần mềm, ý tưởng và thảo luận.

Hackers và luật pháp

Nhìn chung, hầu hết các chính phủ rất lo ngại hacker. Khả năng xâm nhập vào những máy tính không được bảo vệ, ăn trộm thông tin quan trọng nếu chúng thích, là đủ để các cơ quan chính phủ coi đây là ác mộng. Những thông tin bí mật hoặc tin tình báo là cực kì quan trọng. Rất nhiều cơ quan chính phủ không mất thời gian vào việc phân biệt những hacker tò mò muốn thử kỹ năng của mình với hệ thống an ninh bảo mật cao cấp và một gián điệp.

Các điều luận đã thể hiện điều này. Tại Mỹ, có một số luật cấm các hành động hack như 18 U.S.C. § 1029 tập trung vào việc tạo, cung cấp và sử dụng code và các thiết bị giúp hacker truy cập trái phép một hệ thống máy tính. Điều luật này chỉ ghi sử dụng hoặc tạo ra các thiết bị với mục đích lừa gạt, vì vậy, những hacker bị bắt có thể cãi rằng anh ta chỉ sử dụng thiết bị để tìm hiểu cách hoạt động của một hệ thống bảo mật.

Một luật quan trọng khác là 18 U.S.C. § 1030, nghiêm cấm việc truy cập trái phép hệ thống máy tính của chính phủ. Thậm chí, nếu một hacker chỉ

muốn vào thử một hệ thống, người này vẫn phạm luật và bị phạt bởi đã truy cập không công khai máy tính chính phủ.

Việc xử phạt tùy theo mức độ, từ phạt tiền cho tới bỏ tù. Tội nhẹ cũng khiến hacker có thể bị bỏ tù 6 tháng, tội nặng có thể khiến hacker mất 20 năm trong tù. Một công thức từ trang Web của bộ tư pháp Hoa Kỳ dựa trên thiệt hại hoại kinh tế do một hacker gây nên, cùng với số nạn nhân mà người đó gây ra sẽ quyết định án phạt cho hacker này.

Hackers nổi tiếng

Steve Jobs và Steve Wozniak, người sáng lập của Apple, đều là hacker. Một số hành động ban đầu của họ thậm chí còn tương tự với các hành động của hacker nguy hiểm. Tuy nhiên, cả Jobs và Wozniak đã từ bỏ những hành động xấu và tập trung vào việc tạo ra phần mềm và phần cứng máy tính. Nỗ lực của họ đã dẫn đường cho kỷ nguyên máy tính cá nhân – trước Apple, hệ thống máy tính được cho là tài sản của các tập đoàn lớn, rất đắt và cồng kềnh đối với những người thu nhập trung bình.

Linus Torvalds, cha đẻ của Linux, cũng là một hacker nổi tiếng. Hệ điều hành mã nguồn mở của anh ta rất phổ biến với những hacker khác. Anh đã giúp khái niệm phần mềm mã nguồn mở được biết đến nhiều hơn, cho thấy khi bạn mở thông tin đối với mọi người, bạn có thể thu hoạch được rất nhiều lợi ích.

Richard Stallman, thường được viết tắt là RMS, người sáng lập ra dự án GNU, một hệ điều hành miễn phí. Ông là nhà sáng lập ra tổ chức phần mềm tự do FSF và chống lại các điều luật như quản lý quyền kỹ thuật số (Digital Rights Management).

Một trong những hacker mũ đen khác là Jonathan James. Ở tuổi 16, cậu đã trở thành hacker tuổi vị thành niên đầu tiên bị tống vào tù vì tội rình mò bên trong máy chủ của Cơ quan giảm thiểu các mối đe dọa quốc phòng của

Mỹ (DTRA). Jonathan đã cố tình cài đặt một cửa hậu vào trong máy chủ để cho phép mình truy cập vào những email nhạy cảm cũng như tên người dùng, mật khẩu của các nhân viên cơ quan này. Ngoài ra, Jonathan còn tấn công vào Cơ quan Hàng không Vũ trụ Mỹ (NASA) và đánh cắp phần mềm trị giá 1,7 triệu USD. Trên mạng, cậu ta dùng nickname là "c0mrade".

Kevin Mitnick gây được sự chú ý từ những năm 1980 đã đột nhập vào Bộ tư lệnh an ninh phòng không Bắc Mỹ (NORAD) khi mới 17 tuổi. Danh tiếng của Mitnick đã nổi lên cùng với những vụ đột nhập của anh, thậm chí có tin đồn rằng Mitnick đã liệt kê FBI vào danh sách muốn tấn công nhất. Trong đời thường, Mitnick đã bị bắt một vài lần vì tội đột nhập vào hệ thống bảo mật để truy cập các phần mềm máy tính.

Kevin Poulsen, hay Dark Dante, là chuyên gia hack hệ thống điện thoại. Kevin nổi tiếng với vụ hack hệ thống máy chủ điện thoại KIIS-FM. Hành động tin tặc của Poulsen cũng "chẳng giống ai", tấn công vào hầu hết các đường dây điện thoại của Mỹ, làm đảo lộn các số liệu điện thoại ghi trong Yellow Page, hậu quả làm cho nội dung cuộc điện thoại trở nên lộn xộn. Đặc biệt, Poulsen còn can thiệp bằng cách chuyển mạch để chiếm số 102 - số đoạt giải thưởng một chiếc ôtô Porsche 944-S2 trong khuôn khổ chương trình khuyến mại tại khu vực này. Năm 1991, Poulsen bị bắt, bị phạt tù giam 5 năm. Khi mãn hạn tù, Poulsen chuyển sang làm nhà báo và hiện là Tổng biên tập tờ Wired News.

Adrian Lamo hack hệ thống máy tính bằng cách sử dụng các máy tính ở thư viện và các quán café Internet. Anh ta có thể hack những hệ thống lớn để tìm những lỗ hổng bảo mật rồi lợi dụng nó để truy cập vào hệ thống. Sau đó, anh ta lại gửi thông báo tới công ty chủ quản để cho họ biết về lỗ hổng này. Không may cho Lamo, anh ta hoạt động vì sở thích chứ không phải là một chuyên gia được thuê và hành động này là phạm pháp. Ngoài ra, anh ta

cũng đã rình mò quá nhiều, đọc nhiều tài liệu mật và truy cập những tài liệu mật. Anh ta bị bắt sau khi đột nhập vào hệ thống máy tính thuộc thời báo nối tiếng New York Times.

Chúng ta có thể ước chừng có đến hàng ngàn hacker hoạt động trực tuyến, nhưng một con số cụ thể là điều không thể. Rất nhiều hacker không nhận thức rõ điều họ đang làm – họ chỉ đang sử dụng các công cụ nguy hiểm mà bản chất họ cũng hoàn toàn không biết. Số khác biết rõ những gì họ đang làm khi có thể ra, vào một hệ thống mà có thể không ai biết.

2.5.2. Hậu quả mà chúng gây ra.

2015 là một năm đầy bất ổn, không chỉ bởi sự đe dọa của các thế lực khủng bố trên toàn thế giới, mà còn bởi những vụ tấn công của hacker trên mạng internet. Khi mà chúng ta sử dụng mạng internet nhiều hơn và càng có nhiều thiết bị kết nối hơn, mối nguy hiểm này lại càng gia tăng.

Và hậu quả của những vụ hacker tấn công, đánh cắp dữ liệu này là không hề nhỏ. Có thể nó không ảnh hưởng đến sinh mạng của người dân, nhưng những thông tin cá nhân bị đánh cắp có thể gây ra hậu quả nghiêm trọng hơn rất nhiều.

1. Phòng quản lý nhân sự tại Mỹ bị đánh cắp dữ liệu của hơn 20 triệu người

Hồi tháng 6, các hacker đã gây ra một mối đe dọa cực kỳ lớn khi đánh cắp thông tin cá nhân của hơn 20 triệu người dân, từ phòng Quản lý nhân sự Hoa Kỳ. 20 triệu người này bị đánh cắp cả địa chỉ, số an sinh xã hội, email và cả dấu vân tay.

Trong số 20 triệu người này cũng có rất nhiều nhân viên làm việc tại văn phòng Chính phủ Hoa Kỳ. Một số người còn cho biết địa chỉ thư điện tử của họ đã bị xâm phạm và thay đổi. Đây được xem là vụ hacker đánh cắp dữ liệu cá nhân lớn nhất trong lịch sử nước Mỹ.

2. Hacker chiếm quyền điều khiển xe ô tô từ xa

Fiat đã phải thu hồi 1,4 triệu chiếc xe Jeep Grand Cherokee của mình, sau khi tin tặc lợi dụng một lỗ hổng bảo mật của tính năng UConnect để chiếm quyền điều khiển chiếc xe. Các hacker đã sử dụng kết nối di động UConnect và tìm ra địa chỉ IP của chiếc xe, sau đó có thể điều khiển các cuộc gọi, hệ thống giải trí và biến thành một hotspot Wi-Fi.

Nguy hiểm hơn, các hacker có thể cài mã độc vào firmware của hệ thống điều khiển điện tử trên xe, để kiểm soát cả động cơ và hệ thống phanh từ xa.

3. Một tỷ thiết bị Android bị đe dọa do lỗ hổng bảo mật "Stagefright"

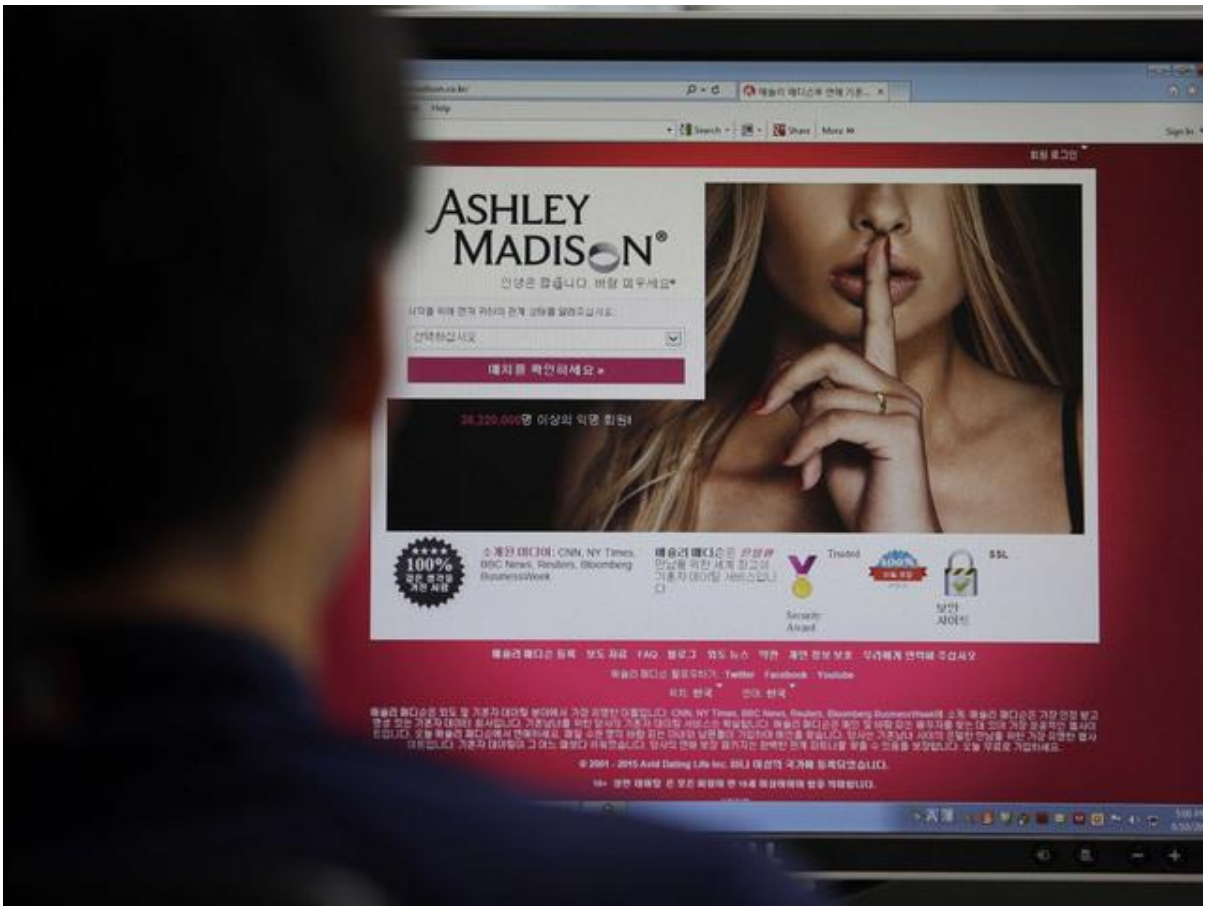
Một lỗ hổng bảo mật có tên là Stagefright đã được phát hiện vào tháng 7, nó cho phép hacker xâm nhập vào thiết bị Android mà người dùng không hay biết. Với hơn 1 tỷ smartphone và tablet Android bị ảnh hưởng, các chuyên gia an ninh đã gọi đây là lỗ hổng bảo mật nguy hiểm nhất từ trước đến nay.

Google đã nhanh chóng tung ra các bản cập nhật để vá lỗi. Tuy nhiên nó vẫn phải thông qua các nhà sản xuất phần cứng để đến được với người dùng, do đó vẫn có thể có hàng triệu thiết bị vẫn đang bị ảnh hưởng bởi lỗ hổng bảo mật này. Rất may là cho đến nay vẫn chưa có báo cáo nào về hậu quả nghiêm trọng do lỗi bảo mật này.

4. Trang web hẹn hò lớn nhất thế giới bị đánh cắp dữ liệu

Trang web hẹn hò ngoại tình Ashley Madison đã bị hacker tấn công và đánh cắp dữ liệu của hơn 32 triệu thành viên. Các dữ liệu bị đánh cắp không

chỉ là tên tuổi, địa chỉ, email mà còn cả thông tin thẻ tín dụng và lịch sử giao dịch.



Vụ hacker tấn công trang web Ashley Madison này đã gây ra rất nhiều hậu quả nghiêm trọng, không chỉ tiết lộ danh tính của những người đã có hành động ngoại tình, mà còn khiến cho kẻ xấu có thể lợi dụng các thông tin này để tống tiền.

. Lỗ hổng bảo mật lớn nhất của Firefox

Trong tháng 8, Mozilla đã cảnh báo người dùng về một lỗ hổng bảo mật của trình duyệt Firefox, có thể được khai thác thông qua một quảng cáo trên một trang web tin tức của Nga. Các lỗ hổng cho phép hacker đánh cắp các tập tin từ máy tính mà người dùng không hay biết.

Không có báo cáo cụ thể về thiệt hại mà lỗ hổng bảo mật này gây ra. Ngay sau đó Mozilla cũng đã nhanh chóng cập nhật một bản vá để khắc phục lỗ hổng này.

. Lỗ hổng bảo mật nghiêm trọng được tìm thấy trong Mac OS

Các sản phẩm của Apple được biết đến với khả năng bảo mật cao nhất, tuy nhiên điều đó không phải là tuyệt đối. Hệ điều hành Mac OS X đã được phát hiện một lỗ hổng bảo mật được gọi là DYLD.

Việc khai thác lỗ hổng bảo mật này cho phép các hacker để cài các mã độc vào máy tính của nạn nhân, mà từ đó có thể đánh cắp nhiều thông tin cá nhân hơn. Apple cũng đã nhanh chóng khắc phục sau khi báo cáo này dược công bố.

7. 15 triệu khách hàng của T-Mobile bị đánh cắp dữ liệu

Trong tháng 10, T-Mobile cho biết đã có khoảng 15 triệu khách hàng đăng ký dịch vụ của nhà mạng này bị đánh cắp các dữ liệu cá nhân nhạy cảm. Tuy nhiên các dữ liệu này không bị đánh cắp trực tiếp từ T-Mobile, mà là từ một bên thứ 3.

Các hacker đã tấn công vào máy chủ của Experian, một dịch vụ giúp kiểm tra thông tin thẻ tín dụng cho T-Mobile. Hacker đã đánh cắp được thông tin cá nhân của 15 triệu khách hàng, trong đó có những thông tin nhạy cảm như tên, địa chỉ, số thẻ ngân hàng và số an sinh xã hội.

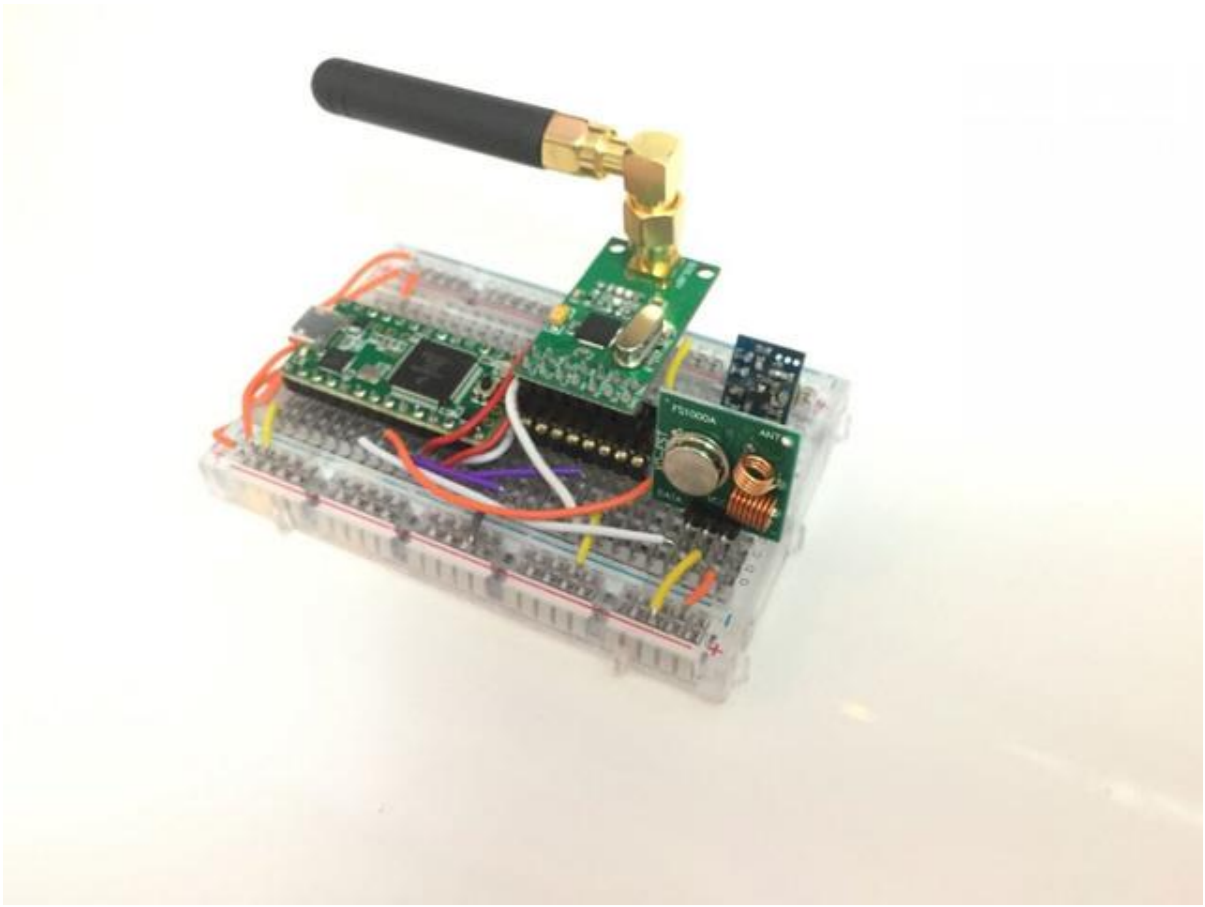
. Dell thừa nhận các dòng laptop của mình bị dính lỗ hổng bảo mật nghiêm trọng

Một lỗ hổng bảo mật đã được Dell xác nhận trên các dòng laptop của mình trong tháng 11 vừa qua. Các lỗ hổng này được phát hiện bên trong một chứng chỉ bảo mật của các laptop được sản xuất từ tháng 8.

Các hacker có thể tận dụng để dẫn người dùng tới các trang web giả mạo, từ đó có thể đánh cắp tài khoản và mật khẩu của người dùng.

. Thiết bị 30 USD có thể mở ổ khóa của bất kỳ chiếc ô tô nào.

Sử dụng các loại linh kiện điện tử được mua trực tuyến với mức giá khoảng 30 USD, một hacker đã tự chế thiết bị có khả năng đột nhập vào bất kỳ nhà để xe và bất kỳ chiếc ô tô nào. Tất cả những gì tên hacker này cần làm chỉ là đặt thiết bị đặc biệt đó lên chiếc xe và mở khóa một cách đơn giản.



Hacker làm được điều đó là nhờ một lỗ hổng của tính năng keyless (mở khóa xe từ xa không cần chìa). Mặc dù tính năng này khá tiện lợi nhưng nó lại rất dễ bị lợi dụng bởi những tên hacker chuyên nghiệp.

. Hàng triệu trẻ em bị đánh cắp thông tin và hình ảnh

Trong tháng 11/2014, Hãng sản xuất đồ chơi VTech của Trung Quốc đã để một lỗ hổng bảo mật tồn tại trong chiếc máy tính bảng dành cho trẻ em của mình. Nó khiến cho các hacker có khả năng đánh cắp thông tin cá nhân của hơn 4,9 triệu tài khoản của phụ huynh và 6,7 triệu tài khoản của trẻ em.

Các thông tin bị đánh cắp gồm cả tên, địa chỉ, email, các mật khẩu đã bị mã hóa, địa chỉ IP và nhiều thông tin khác. Tuy nhiên nghiêm trọng nhất là cả những bức ảnh chụp của trẻ cũng bị đánh cắp và nó có thể dẫn đến những mối đe dọa nguy hiểm hơn, như bắt cóc tống tiền.

2.6. Tấn công mạng

Đối với các cuộc tấn công bằng việc khai thác các lỗ hổng, yêu cầu các hacker phải hiểu biết về các vấn đề bảo mật trên hệ điều hành hoặc các phần mềm và tận dụng kiến thức này để khai thác các lỗ hổng.

***Tấn công bị động (Passive attack*)**

Trong một cuộc tấn công bị động, các hacke sẽ kiểm soát traffic không được mã hóa và tìm kiếm mật khẩu không được mã hóa (Clear Text password), các thông tin nhạy cảm có thể được sử dụng trong các kiểu tấn công khác. Các cuộc tấn công bị động bao gồm phân tích traffic, giám sát các

cuộc giao tiếp không được bảo vệ, giải mã các traffic mã hóa yếu, và thu thập các thông tin xác thực như mật khẩu.

Các cuộc tấn công chặn bắt thông tin hệ thống mạng cho phép kẻ tấn công có thể xem xét các hành động tiếp theo. Kết quả của các cuộc tấn công bị động là các thông tin hoặc file dữ liệu sẽ bị rơi vào tay kẻ tấn công mà người dùng không hề hay biết.

Tấn công phân tán (Distributed attack)

Đối với các cuộc tấn công rải rác yêu cầu kẻ tấn công phải giới thiệu mã, chẳng hạn như một chương trình Trojan horse hoặc một chương trình back-door, với một thành phần "tin cậy" hoặc một phần mềm được phân phối cho nhiều công ty khác và tấn công user bằng cách tập trung vào việc sửa đổi các phần mềm độc hại của phần cứng hoặc phần mềm trong quá trình phân phối,... Các cuộc tấn công giới thiệu mã độc hại chẳng hạn như back door trên một sản phẩm nhằm mục đích truy cập trái phép các thông tin hoặc truy cập trái phép các chức năng trên hệ thống.

Tấn công nội bộ (Insider attack)

Các cuộc tấn công nội bộ (insider attack) liên quan đến người ở trong cuộc, chẳng hạn như một nhân viên nào đó "bất mãn" với công ty của mình,…các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại.

Người trong cuộc cố ý nghe trộm, ăn cắp hoặc phá hoại thông tin, sử dụng các thông tin một cách gian lận hoặc truy cập trái phép các thông tin.

Tấn công Phishing

Trong các cuộc tấn công phishing, các hacker sẽ tạo ra một trang web giả trông "giống hệt" như các trang web phổ biến. Trong các phần tấn công phishing, các hacker sẽ gửi một email để người dùng click vào đó và điều hướng đến trang web giả mạo. Khi người dùng đăng nhập thông tin tài khoản của họ, các hacker sẽ lưu lại tên người dùng và mật khẩu đó lại.

Các cuộc tấn công của không tặc (Hijack attack)

Trong các cuộc tấn công của không tặc, các hacker sẽ giành quyền kiểm soát và ngắt kết nối cuộc nói chuyện giữa bạn và một người khác.

Tấn công mật khẩu (Password attack)

Đối với các cuộc tấn công mật khẩu, các hacker sẽ cố gắng "phá" mật khẩu được lưu trữ trên cơ sở dữ liệu tài khoản hệ thống mạng hoặc mật khẩu bảo vệ các tập tin.

Các cuộc tấn công mật khẩu bao gồm 3 loại chính: các cuộc tấn công dạng từ điển (dictionary attack), brute-force attack và hybrid attack.

Cuộc tấn công dạng từ điển sử dụng danh sách các tập tin chứa các mật khẩu tiềm năng.

. Khai thác lỗ hổng tấn công (Exploit attack)

Đối với các cuộc tấn công bằng việc khai thác các lỗ hổng, yêu cầu các hacker phải hiểu biết về các vấn đề bảo mật trên hệ điều hành hoặc các phần mềm và tận dụng kiến thức này để khai thác các lỗ hổng.

. Buffer overflow (lỗi tràn bộ đệm)

Một cuộc tấn công buffer attack xảy ra khi các hacker gửi dữ liệu tới một ứng dụng nhiều hơn so với dự kiến. Và kết quả của cuộc tấn công buffer attack là các hacker tấn công truy cập quản trị hệ thống trên Command Prompt hoặc Shell.

. Tấn công từ chối dịch vụ (denial of service attack)

Không giống như các cuộc tấn công mật khẩu (Password attack), các cuộc tấn công từ chối dịch vụ (denial of service attack) ngăn chặn việc sử dụng máy tính của bạn hoặc hệ thống mạng theo cách thông thường bằng valid users.

Sau khi tấn công, truy cập hệ thống mạng của bạn, các hacker có thể:

- Chặn traffic.

- Gửi các dữ liệu không hợp lý tới các ứng dụng hoặc các dịch vụ mạng, dẫn đến việc thông báo chấm dứt hoặc các hành vi bất thường trên các ứng dụng hoặc dịch vụ này.

- Lỗi tràn bộ nhớ đệm.

. Tấn công theo kiểu Man-in-the-Middle Attack

Đúng như cái tên của nó, một cuộc tấn công theo kiểu Man-in-the-Middle Attack xảy ra khi cuộc nói chuyện giữa bạn và một người nào đó bị kẻ

tấn công theo dõi, nắm bắt và kiểm soát thông tin liên lạc của bạn một cách minh bạch.

Các cuộc tấn công theo kiểu Man-in-the-Middle Attack giống như một người nào đó giả mạo danh tính để đọc các tin nhắn của bạn. Và người ở đầu kia tin rằng đó là bạn, bởi vì kẻ tấn công có thể trả lời một cách tích cực để trao đổi và thu thập thêm thông tin.

. Tấn công phá mã khóa (Compromised-Key Attack)

Mã khóa ở đây là mã bí mật hoặc các con số quan trọng để "giải mã" các thông tin bảo mật. Mặc dù rất khó để có thể tấn công phá một mã khóa, nhưng với các hacker thì điều này là có thể. Sau khi các hacker có được một mã khóa, mã khóa này sẽ được gọi là mã khóa gây hại.

Hacker sử dụng mã khóa gây hại này để giành quyền truy cập các thông tin liên lạc mà không cần phải gửi hoặc nhận các giao thức tấn công. Với các mã khóa gây hại, các hacker có thể giải mã hoặc sửa đổi dữ liệu.

. Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò tìm tên người sử dụng và mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà vv.. để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một chương trình tự động hoá về việc dò tìm mật khẩu này.

Một chương trình có thể dễ dàng lấy được từ Internet để giải các mật khẩu đã mã hoá của hệ thống unix có tên là crack, có khả năng thử các tổ hợp các từ trong một từ điển lớn, theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp này có thể lên tới 30%.

Phương pháp sử dụng các lỗi của chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được tiếp tục để chiếm quyền truy nhập. Trong một số trường hợp phương pháp này cho phép kẻ tấn công có được quyền của người quản trị hệ thống (root hay administrator).

Hai ví dụ thường xuyên được đưa ra để minh hoạ cho phương pháp này là ví dụ với chương trình sendmail và chương trình rlogin của hệ điều hành UNIX.

Sendmail là một chương trình phức tạp, với mã nguồn bao gồm hàng ngàn dòng lệnh của ngôn ngữ C. Sendmail được chạy với quyền ưu tiên của người quản trị hệ thống, do chương trình phải có quyền ghi vào hộp thư của những người sử dụng máy. Và Sendmail trực tiếp nhận các yêu cầu về thư tín

trên mạng bên ngoài. Đây chính là những yếu tố làm cho sendmail trở thành một nguồn cung cấp những lỗ hổng về bảo mật để truy nhập hệ thống.

Rlogin cho phép người sử dụng từ một máy trên mạng truy nhập từ xa vào một máy khác sử dụng tài nguyên của máy này. Trong quá trình nhận tên và mật khẩu của người sử dụng, rlogin không kiểm tra độ dài của dòng nhập, do đó kẻ tấn công có thể đưa vào một xâu đã được tính toán trước để ghi đè lên mã chương trình của rlogin, qua đó chiếm được quyền truy nhập.

. Nghe trộm

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên, mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa card giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

. Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source-routing). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

. Vô hiệu các chức năng của hệ thống

Đây là kiểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

Ví dụ sử dụng lệnh ping với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

. Lỗi của người quản trị hệ thống

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

. Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác.

Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

Kết luận. Chương 2. trình bày các lỗ hổng bảo mật cơ bản mà các hacker thường lợi dụng để thực hiện để tấn công vào các mạng máy tính cục bộ hoặc các máy tính cá nhân theo ý đồ của chúng.

Chương 3. ĐỀ XUẤT KỸ THUẬT PHÒNG VÀ PHÁT HIỆN XÂM NHẬP MẠNG

3.1. Một số kỹ thuật phòng thủ

3.1.1 *Firewall*

Firewall là giải pháp bảo vệ mạng hiệu quả và phổ biến nhất hiện nay. Sau đây ta sẽ tìm hiểu về khái niệm, chức năng và phân loại firewall.

3.1.1.1 Khái niệm firewall.

Firewall là thiết bị ngăn chặn sụ truy cập không hợp lệ từ mạng bên ngoài vào mạng bên trong. Firewall bao gồm cả phần cứng và phần mềm.

31.1.2 Các chức năng cơ bản của firewall.

Firewall cho phép ngăn chặn dịch vụ từ trong ra ngoài và ngược lại; Kiểm soát địa chỉ truy cập và dịch vụ sử dụng; Kiểm soát khả năng truy cập; Kiểm soát nội dung thông tin truyền tải; Ngăn ngừa tấn công từ các mạng bên ngoài.

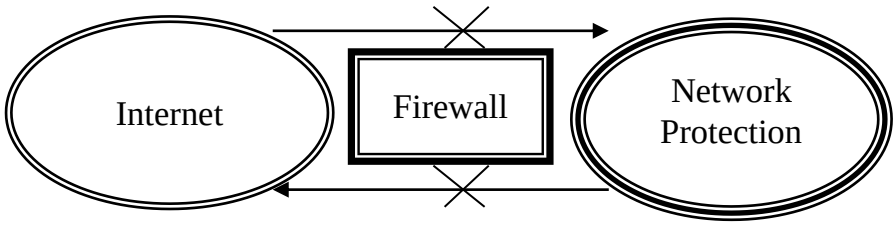
3.1.1.3 Phân loại firewall.

Firewall có nhiều loại khác nhau và mỗi loại có ưu nhược điểm riêng. Thông thường firewall được chia làm 2 loại: firewall phần cứng và firewall phần mềm

a. Firewall phần cứng:

Là thiết bị được tích hợp bộ định tuyến, quy tắc lọc gói tin được đặt trên bộ định tuyển.

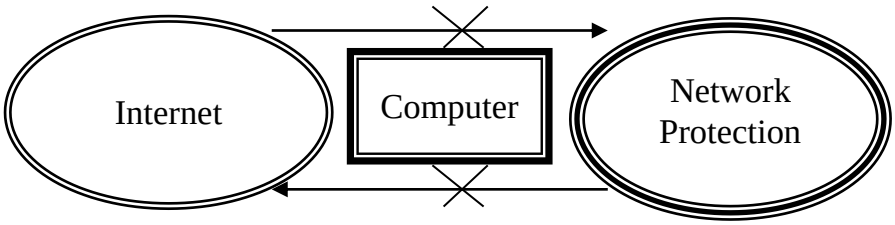
Firewall sẽ dựa trên nguyên tắc để kiểm tra gói tin. Mô hình firewall phần cứng (Hình 3-1)



Hình 3.1. Mô hình Firewall phần cứng

b. Firewall phần mềm:

Là phần mềm cho phép chuyển các gói tin mà máy chủ nhận được đến địa điểm theo yêu cầu, các quy tắc thiết lập gói tin được người sử dụng tự thiết lập. Mô hình fĩrewall phần cứng (Hình 3-2)



Hình 3.2. Mô hình Firewall phần mềm

c. Ưu và nhược điểm của firewall:

Firewall phần cứng thường được sử dụng cho các mạng lớn, fĩrewall nhận gói tin và kiểm duyệt rồi chuyển tiếp cho các máy trong mạng, tốc độ của firewall phần mềm hoạt động chậm hơn so với fĩrewall phần cứng nên ảnh hưởng đến tốc độ của hệ thống mạng.

Firewall phần mềm sử dụng để đảm bảo anh ninh cho các mạng vừa, nhỏ do đó chi phí thấp, không ảnh hưởng đến tốc độ chuyển các gói tin; Firewall phần mềm thực hiện trên từng hệ điều hành nhất định. Firewall phần cứng có thể thực hiện độc lập.

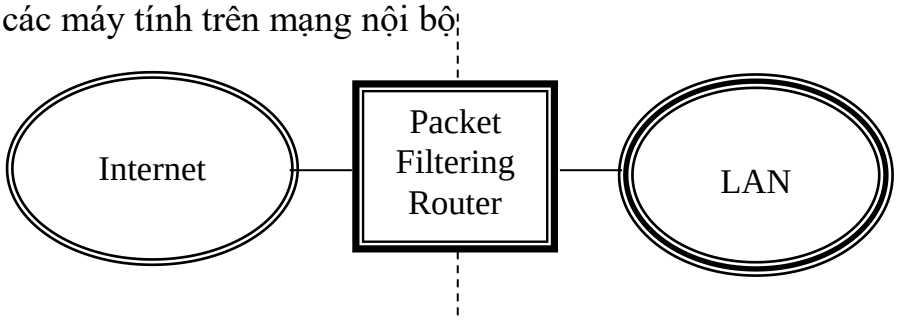
Firewall phần mềm có thể lọc được nội dung gói tin còn fĩrewall phần cứng chỉ có thể lọc thông tin của gói tin, nội dung của gói tin thì firewall phần cứng không thể kiểm soát.

3.1.1.4. Một số hệ thống fĩrewall khác.

a. Packet-Filtering Router (Bộ định tuyến có lọc gói) - Hình 3-3.

Có hai chức năng: chuyển tiếp thông tin giữa hai mạng và sử dụng các quy luật về lọc gói để cho phép hay từ chối truyền thông. Quy luật lọc được định nghĩa sao cho các host trên mạng nội bộ được quyền truy cập trực tiếp

tới internet, trong khi các host trên internet chỉ có một số giới hạn các truy cập vào các máy tính trên mạng nội bộ



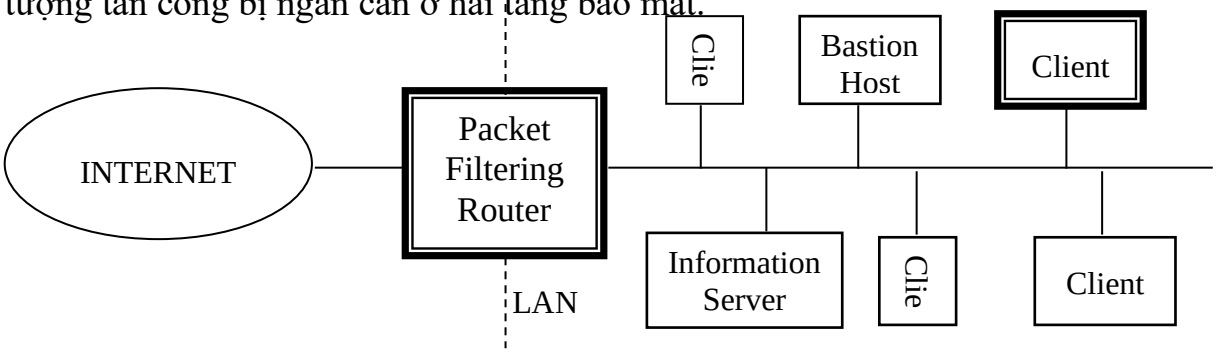
Hình 3-3: Mô hình sử dụng Packet - Filtering Router

Ưu điểm: cấu hình đơn giản, chi phí thấp; Trong suốt đối với người dùng.

Hạn chế: Dễ bị tấn công vào các bộ lọc do cấu hình không hoàn hảo.

b. Screened Host Firewall - Hình 3-4.

Bao gồm một Packet-Filtering Router và một Bastion Host. Screened Host Firewall cung cấp độ bảo mật cao hơn Packet-Filtering Router, vì hệ thống thực hiện bảo mật ở tầng mạng và tầng ứng dụng. Mô hình này, đối tượng tấn công bị ngăn cản ở hai tầng bảo mật.



Hình 3-4: Mô hình Screen Host Firewall

c.Delimitarized Zone (DMZ - khu vực phi quân sự) - Hình 3-5.

Bao gồm hai Packet-Filtering Router và một Bastion Host, có độ an toàn cao nhất vì cung cấp cả mức bảo mật mạng và ứng dụng. Mạng DMZ đóng vai trò độc lập đặt giữa internet và mạng nội bộ, được cấu hình sao cho các hệ thống chỉ có thể truy cập được một số dịch vụ mà không thể kết nối trực tiếp với mạng DMZ.

Ưu điểm: Ba tầng bảo vệ: Router ngoài, Bastion host và Router trong.

3.1.1.5. Các kiến trúc firewall

a. Kiến trúc Dual-Home Host.

Phải có ít nhất hai card mạng giao tiếp với hai mạng khác nhau và đóng vai trò router mềm; Kiến trúc này rất đơn giản, Dual-Home Host ở giữa, một bên được kết nối với internet và một bên kết nối với mạng LAN.

b. Kiến trúc Screen Host.

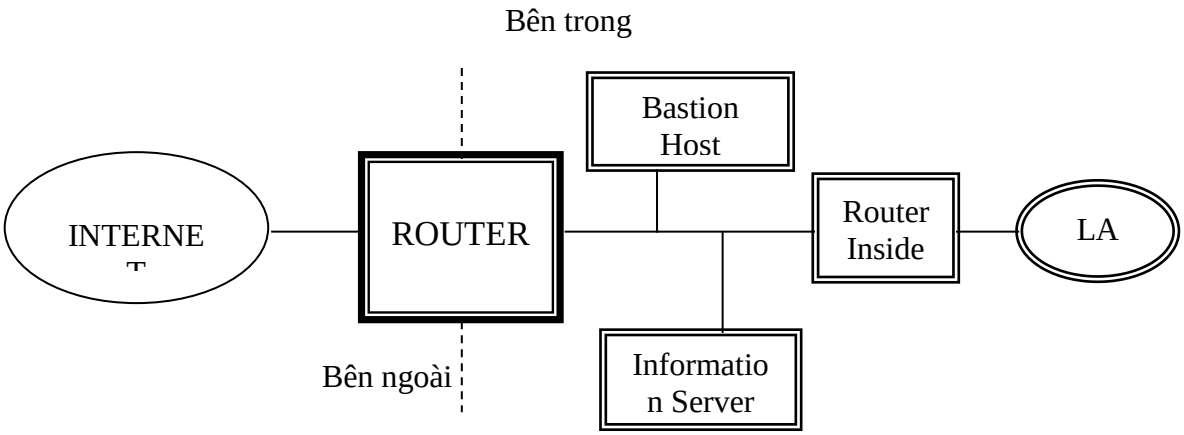
Có cấu trúc ngược lại với Dual-Home Host, cung cấp dịch vụ từ một host trong mạng nội bộ, dùng một router độc lập với mạng bên ngoài, cơ chế bảo mật của kiến trúc này là phương pháp Packet Filtering.

c. Kiến trúc Screen Subnet (Hình 3-5).

Kiến trúc này dựa trên nền tảng của kiến trúc Screen Host bằng cách thêm vào phần an toàn nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách Bastion Host ra khỏi các host thông thường khác. Kiểu Screen Subnet đơn giản gồm hai Screen Router:

- Router ngoài: Nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi.

- Router trong: Nằm giữa mạng ngoại vi và mạng nội bộ, nằm bảo vệ mạng nội bộ trước khi ra với bên ngoài và mạng ngoại vi.



Hình 3-5: Mô hình Screened-subnetflrewall

3.1.1.6. Chính sách xây dựng firewall.

Một số giải pháp và nguyên tắc cơ bản khi xây dựng firewall

a. Quyền hạn tối thiểu (Least Privilege)

Nguyên tắc này có nghĩa là bất cứ một đối tượng nào bên trong hệ thống chỉ nên có những quyền hạn nhất định.

b. Bảo vệ theo chiều sâu (Defense in Depth).

Lắp đặt nhiều cơ chế an toàn để có thể hỗ trợ lẫn nhau. Vì vậy firewall được xây dựng theo cơ chế có nhiều lớp bảo vệ là hợp lý nhất.

c. Nút thắt (Choke Point).

Một nút thắt bắt buộc những kẻ đột nhập phải đi qua một ngõ hẹp mà người quản trị có thể kiểm soát.

d. Điểm xung yếu nhất (Weakest Link).

Cần phải tìm ra những điểm yếu của hệ thống để có phương án bảo vệ, tránh đối tượng tấn công lợi dụng để truy cập trái phép

e. Hỏng trong an toàn (Fail-Safe Stance).

Nếu hệ thống đang hỏng thì phải hỏng theo một cách nào đó để ngăn chặn sự truy cập bất hợp pháp tốt hơn là để cho kẻ tấn công lọt vào phá hệ thống.

f. Sự tham gia toàn cầu.

Các hệ thống mạng phải có biện pháp bảo vệ an toàn. Nếu không, đối tượng truy cập bất hợp pháp có thể truy cập vào hệ thống này, sau đó truy cập sang hệ thống khác.

g. Tính đa dạng của việc bảo vệ.

Áp dụng nhiều biện pháp bảo vệ thông tin dữ liệu trong hệ thống mạng theo chiều sâu.

h. Tuân thủ các nguyên tắc căn bản (Rule Base).

Thực hiện theo một số quy tắc nhất định, khi có một gói tin đi qua

firewall thì phải dựa vào các quy tắc đề ra để phân tích và lọc gói tin.

i. Xây dựng chỉnh sách an toàn (Security Policy).

Firewall phải được thiết kế, xây dựng bằng một chính sách an toàn sẽ tạo ra được sức mạnh và hiệu quả. Một số chính sách an toàn như sau:

- Hạn chế những máy trong mạng nội bộ được truy cập internet.

- Thông tin vào ra trong mạng nội bộ đều phải được xác thực và mã hóa.

j. Thứ tự các quy tắc trong bảng (Sequence of Rule Base)

Cần phải quan tâm đến thứ tự, cấp độ của quy tắc và trong đó có một số quy tắc đặc biệt. Đa số các flrewall kiểm tra các gói tin một cách tuần tự và liên tục, khi firewall nhận một gói tin, nó sẽ kiểm tra gói tin đó có đúng với nguyên tắc hay không cho đến khi có quy tắc nào thỏa mãn thì nó thực thi theo quy tắc đó.

k. Các quy tắc căn bản (Rule Base).

Không có gói tin nào có thể đi qua được, bất kể gói tin đó là gì.

- Đầu tiên cho phép đi từ trong ra ngoài mà không có hạn chế nào.

- Hạn chế tất cả không có phép một sự xâm nhập nào vào flrewall.

- Không ai có thể kết nối với firewall, bao gồm cả Admin, phải tạo ra một quy tắc đế cho phép Admin truy cập được vào firewall.

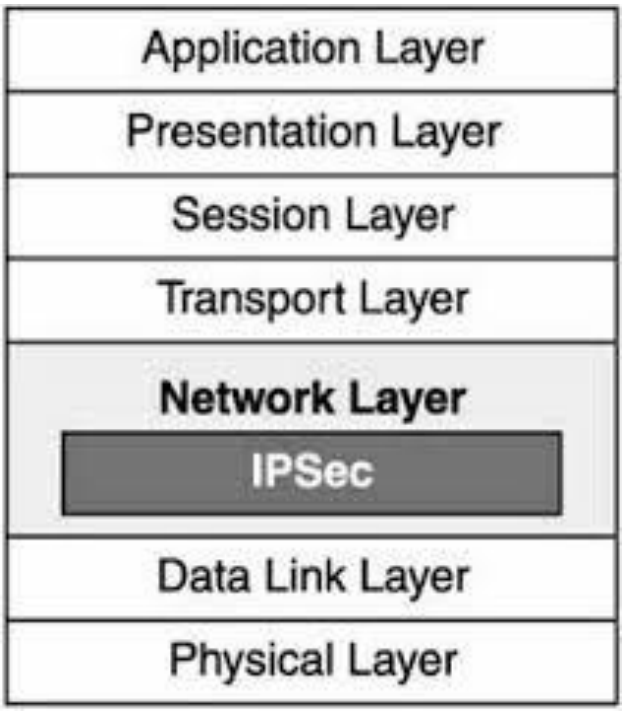
3.1.2 IP Security.

3.1.2.1. Tổng quan.

IPSec (IP Security) bao gồm các giao thức để bảo mật quá trình truyền thông tin trên nền tảng Internet Protocol (IP). Gồm xác thực và/hoặc mã hóa (Authenticating, Encrypting) cho mỗi gói IP (IP Packet) trong quá trình truyền thông tin. Giao thức IPSec được làm việc tại tầng Network Layer của mô hình OSI - Hình 3-6.

3.1.2.2. Cấu trúc bảo mật.

Khi IPSec được triển khai, Cấu trúc bảo mật của nó gồm: Sử dụng các giao thức cung cấp mật mã nhằm bảo mật gói tin; Cung cấp phương thức xác thực; Thiết lập các thông số mã hóa.



Hình 3-6:Mô hình OSI (Open System Interconnection)

3.1.2.3. Thực trạng

IPSec là một phần bắt buộc của Ipv6, có thể được lựa chọn khi sử dụng Ipv4. Trong khi các chuẩn đã được thiết kế cho các phiên bản IP giống nhau, phổ biến nhất hiện nay là áp dụng và triển khai trên nền tảng Ipv4.

3.1.2.4. Thiết kế theo yêu cầu.

IPSec được cung cấp bởi Transport Mode (End-to-End) đáp ứng bảo mật giữa các máy tính giao tiếp trực tiếp với nhau hoặc sử dụng Tunnel Mode (Portal-to-Portal) cho các giao tiếp giữa hai mạng với nhau và chủ yếu được sử dụng khi kết nối VPN. IPSec đã được giới thiệu và cung cấp các dịch vụ bảo mật:

-Mã hóa quá trình truyền thông tin; Đảm bảo tính nguyên vẹn của dữ

liệu; Được xác thực giữa các giao tiếp; Chống quá trình Replay trong các phiên bảo mật; Modes - Các mode.

-Có hai mode thực hiện IPSec đó là:

+ Transport Mode: Chỉ những dữ liệu giao tiếp các gói tin được mã hóa và/hoặc xác thực.

+ Tunnel Mode: Toàn bộ gói IP được mã hóa và xác thực.

3.1.2.5. Mô tả kỹ thuật.

Có hai giao thức cung cấp để bảo mật cho gói tin của cả hai phiên bản Ipv4 và Ipv6:

-IP Authentication Header: Giúp đảm bảo tĩnh toàn vẹn và cung cấp xác thực.

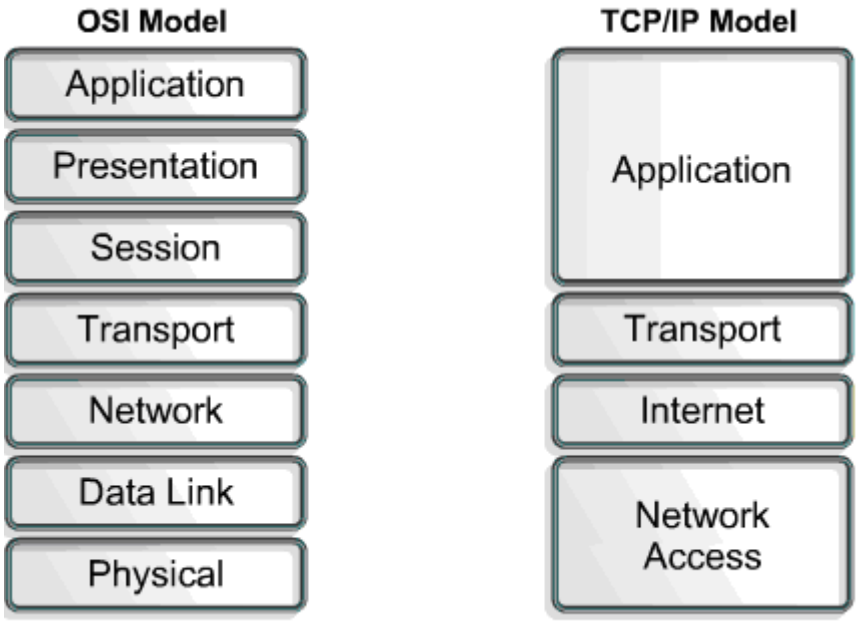
-IP Encapsolating Security Payload: Cung cấp bảo mật và có thể lựa chọn cả tính năng Authentication và Integrity để đảm bảo tính toàn vẹn dữ liệu.

a. Giao thức Authentication Header (AH).

AH dược sử dụng trong các kết nối không có tính đảm bảo dữ liệu. Là lựa chọn nhằm chống lại các tấn công Replay Attaclc bằng cách sử dụng công nghệ tấn công Sliding Windows và Discarding Older Packets. Hình 3-7 là mô tả của AH.

Các Model thực hiện:

- Next Header: Nhận dạng giao thức trong sử dụng truyền thông tin.
- Payload Length: Độ lớn của gói tin AH.
- Reserved: Sử dụng trong tương lai (được biểu diễn bằng các số 0).



Hình 3-7: Mô hình hoạt động trong giao thức AH

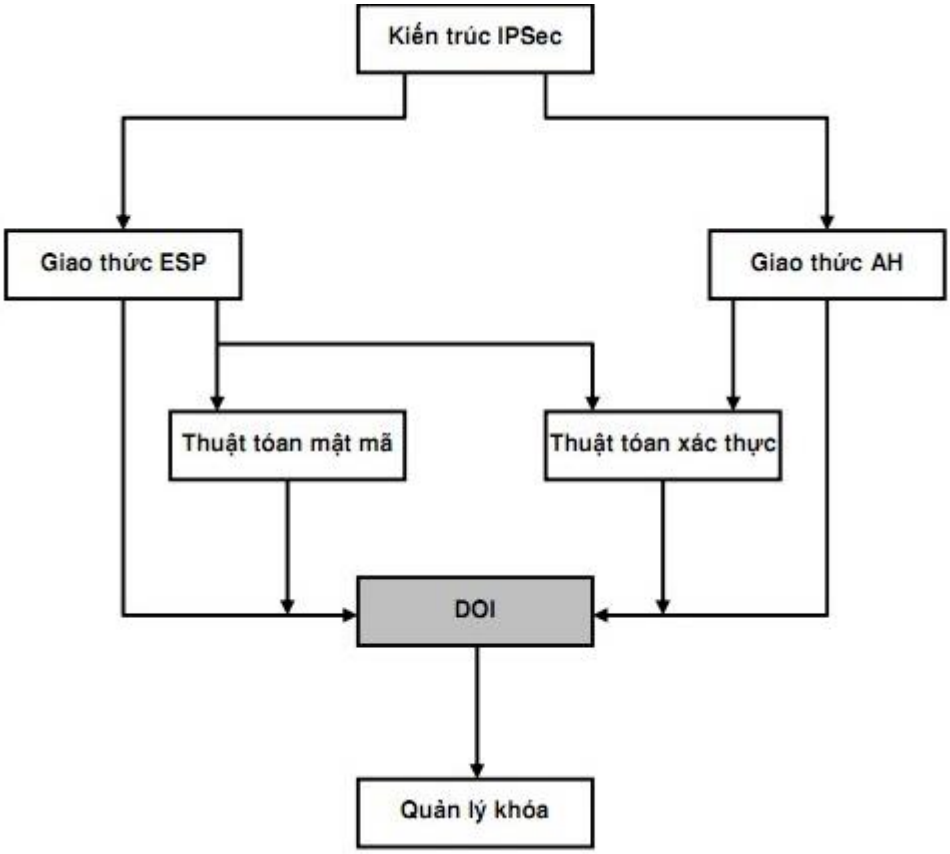
- Security Parameter Index (SPI): Nhân ra các thông số bảo mật, được tích hợp với IP, và nhận dạng các thương lượng bảo mật đượv kết hợp với gói.tin.

- Sequence Number: Một số tự động tăng lên mỗi gói tin, sử dụng nhằm chống lại tấn công dạng replay attack.

- Authentication Data: Bao gồm thông số Integrity Check Value (ICV) cần thiết trong gói tin xác thực.

b.Encapsolating Security Payload (ESP) - Hình 3-8.

Giao thức ESP cung cấp xác thực, toàn vẹn, bảo mật cho gói tin. ESP cũng hỗ trợ tính năng cấu hình sử dụng trong trường hợp chỉ cần mã hóa và chỉ cần Authentication, nhưng sử dụng mã hóa mà không yêu cầu xác thực không đảm bảo tính bảo mật.



Hình 3-8: Mô hình hoạt động trong giao thức ESP.

Các Model thực hiện:

- Security Parameter Index (SPI): Nhân ra các thông số được tích hợp với IP.

- Sequence Number: Một số tự động tăng có tác dụng chống lại tấn công dạng

replay

- Payload Data: Cho dữ liệu truyền đi.

- Padding: Sử dụng vài Block mã hóa.

- Pad Length: Độ lớn của Padding.

- Next Header: Nhận ra giao thức được sử dụng trong khi truyền thông tin.

- Authentication Data: Bao gồm dữ liệu để xác thực gói tin,

3.1.2.6. Thực hiện.

IPSec được thực hiện trong nhân với các trình quản lý các khóa và quá trình thỏa hiệp bảo mật ISAKMP/IKE từ người dùng. Tuy nhiên một chuẩn giao diện cho quản lý khóa, nó có thể được diều khiển bởi nhân của IPSec

3.1.3. Mã hóa công khai và chứng thực thông tin.

3.1.3.1. Tổng quan về cơ sở hạ tầng mã hóa công khai (Public Key Infrastructure - PKI).

* Khái niệm hạ tầng cơ sở mật mã khóa công khai.

Là cơ chế cho một bên thứ 3 cung cấp và xác định định danh các bên tham gia vào quá trình trao đổi thông tin. Mục tiêu của PKI là cho phép những người tham gia xác thực lẫn nhau và sử dụng thông tin từ các chứng thực khóa công khai để mã hóa và giải mã thông tin.

* Các dịch vụ và phạm vi ứng dụng của PKI.

a. Các dịch vụ của PKI có khả năng đảm bảo 5 yếu tố sau:

- Bảo mật thông tin: Các thực thể không được cấp quyền thì khó có thể xem bản tin.

- Toàn vẹn thông tin: Đảm bảo cho thông tin khó bị thay đổi bởi các thực thể không được cấp quyền.

- Xác thực thực thể: Các thực thể nhận bản tin biết giao dịch với thực thể nào.

- Chống chối bỏ: Các thực thể không thể chối bỏ những hành động đã thực hiện.

- Tính pháp lý: Thông tin phải ở dạng cố định được ký bởi tất cả các bên hợp pháp và phải cho phép thực hiện thẩm tra.

b. Phạm vi ứng dụng của PKI.

- PKI được cho là giải pháp hữu hiệu hiện nay trong việc đảm bảo an ninh an toàn cho hệ thống thông ti.

- Phạm vi ứng dụng của PKI bao gồm: Mã hóa email hoặc xác thực người gửi email; Mã hóa hoặc nhận thực văn bản; Xác thực người dùng ứng dụng; Các giao thức truyền thông an toàn trao đổi khóa bằng khóa bất đối xứng, còn mã hóa bằng bất đối xứng.

c. Các thành phần phần của PKI

PKI bao gồm 3 thành phần chính:

-Phần 1: Tập hợp các công cụ, phương tiện, các giao thức đảm bảo an toàn thông tin.

-Phần 2: Hành lang pháp lý là luật, các qui định dưới luật về giao dịch điện tử.

-Phần 3: Các tổ chức điều hành giao dịch điện tử (CA, RA,...).

d. Một sỗ chức năng của PKI.

➢ Quản lý khóa.

- Sinh khóa:

Khóa sinh ra phải đảm bảo về chất lượng. Có 2 cái mà hệ thống sử dụng khóa để tạo khóa:

+ Người sử dụng tự sinh cặp khóa cho mình sau đó gửi khóa công khai cho tô chức cấp giấy chứng nhận (Certification Authority - CA).

+ Cặp khóa sinh bởi một hệ thống chuyên chịu trách nhiệm sinh khóa. Khóa công khai được gửi cho CA quản lý, khóa bí mật được gửi cho người dùng theo một kênh an toàn.

- Phân phối và thu hồi khóa:

+ Phân phối khóa; Thông qua các kênh truyền thông cần đảm bảo an toàn. Khóa bí mật được phân phối cho người dùng thông qua các kênh truyền an toàn.

+ Thu hồi, treo khóa: Thông qua việc thu hồi chứng chỉ, là quá trình thu hồi khóa tạm thời, khóa đó có thể được sử dụng lại.

- Cập nhật thông tin về cặp khóa:

+ Cặp khóa của các đối tượng tharn gia vào hệ thống PKI cần phải được cập nhật một cách thường xuyên, vì các cặp khóa có thể được thay đổi bằng cặp khóa mới.

- Cập nhật thông tin về cặp khóa của CA:

Cũng giống như sử dụng chứng chỉ, cặp khóa của CA được cập nhật thường xuyên

- Khôi phục khóa:

Hầu hết hệ thống PKI tạo ra hai cặp khóa cho người sử dụng cuối, một để ký số và một để mã hóa để sao lưu dự phòng khóa.

* Quản lý chứng chỉ.

-Đăng ký và xác nhận ban đầu.

CA sẽ cấp cho đối tượng đăng ký một chứng chỉ số và gửi chứng chỉ số này cho hệ thống lưu trữ.

- Cập nhật thông tin về chứng chỉ số.

Mỗi chứng chỉ số chỉ có tác dụng trong khoảng thời gian nhất định. Khi các chứng chỉ số hết hạn, CA sẽ tạo một chứng chỉ số mới và cập nhật thông tin về chứng chỉ số này.

-Phát hành chứng chỉ và danh sách chứng chỉ bị hủy bỏ.

Khi CA phát hành một chứng chỉ số, trước hết nó phải dựa trên định dạng của chứng chỉ số cần cấp. Sau khi có được danh sách các thông tin về chính sách quản trị, CA sẽ tổ chức chúng theo định dạng đã biết, khi đó chứng chỉ số mới hoàn thiện.

-Hủy bỏ chứng chỉ số.

Hệ thống PKI sẽ thực hiện hủy bỏ chứng chỉ số nếu đối tượng sử dụng chứng chỉ số bị phát hiện có những dấu hiệu sử dụng phạm pháp.

- Quản lý thời gian.

Thời gian trong hệ thống PKI có tính nhất quán, đồng bộ giữa tất cả các thành phần.

- Giao tiếp giữa các PKI.

Các thành phần trong hệ thống giao tiếp được với nhau, các hệ thống PKI khác cũng có thể giao tiếp được như các thành phần khác trong cùng hệ thống.

e. Các thành phần đảm bảo an toàn thông tin.

- Kỹ thuật bảo mật thông tin: Hệ mã hóa thường được sử dụng nhất trong cá hệ PKI phục vụ bảo mật thông tin là hệ mã hóa công khai RSA.
- Kỹ thuật xác thực: Sử dụng sơ đồ chữ ký RSA.

f. Hệ thống cung cấp và quản lý chứng chỉ số.

* Chứng chỉ số (Hình 3-12).

- Khái niệm.

Chứng chỉ số là một dạng kết hợp giữa 3 thành phần:

+ Các thông tin mô tả về bản thân đối tượng: số định danh, tên, địa chỉ email, loại chứng chỉ, hạn sử dụng, phạm vi áp dụng...

+ Khóa công khai tương ứng.

+ Chữ ký điện tử của các cơ quan cấp phát chứng chỉ số cho các thông tin trên.

- Mục đích và yd nghĩa của chứng chỉ số.

+ Mã hóa thông tin: Lợi ích đần tiên của chứng chỉ số là tính an toàn bảo mật thông tin.

+ Chống giả mạo: Khi gửi đi một thông tin có sử dụng chứng chỉ số, người nhận có thể kiểm tra được thông tin của người gửi có bị thay đổi hay không.

+ Xác thực: Khi gửi một thông tin giao dịch đính kèm chứng chỉ số, người nhận sẽ xác định rõ được danh tính của người gửi.

+ Chống từ chối: Khi sử dụng một chứng chỉ số, người gửi phải chịu hoàn toàn trách nhiệm về những thông tin mà chứng chỉ số đi kèm.

- Chứng chỉ khóa công khai X. 509.

+ Sử dụng phổ biến trong hầu hết các hệ thống PKI. Chứng chỉ X.509 v3 là định dạng chứng chỉ được sử dụng phổ biến và được nhà cung cấp PKI triển khai.

+ Có 6 trường hợp bắt buộc là:

- ✓ Số phát hành (Serial Number).
- ✓ Kỹ thuật mã hóa ký số (Certificate Signature Algorithm Identifier). Tên của CA phát hành chứng chỉ (Certificate Issuer Name).
- ✓ Thời hạn hiệu lực của chứng chỉ (Certificate Validity Period).
- ✓ Khóa công khai (Public Key).
- ✓ Tên của chủ thể (SubjectName).

- Danh sách chứng chỉ thu hồi

+ Các chứng chỉ này có chứa ngày hết hạn hiệu lực. Khi cần thu hồi một chứng chỉ trước thời hạn, người phát hành cần một phương tiện để cập nhật thông tin trạng thái chứng chỉ của mọi chứng chỉ cho người dùng.

+ Danh sách chứng chỉ thu hôi X.509 được bảo vệ bởi chữ ký số của CA phát hành.

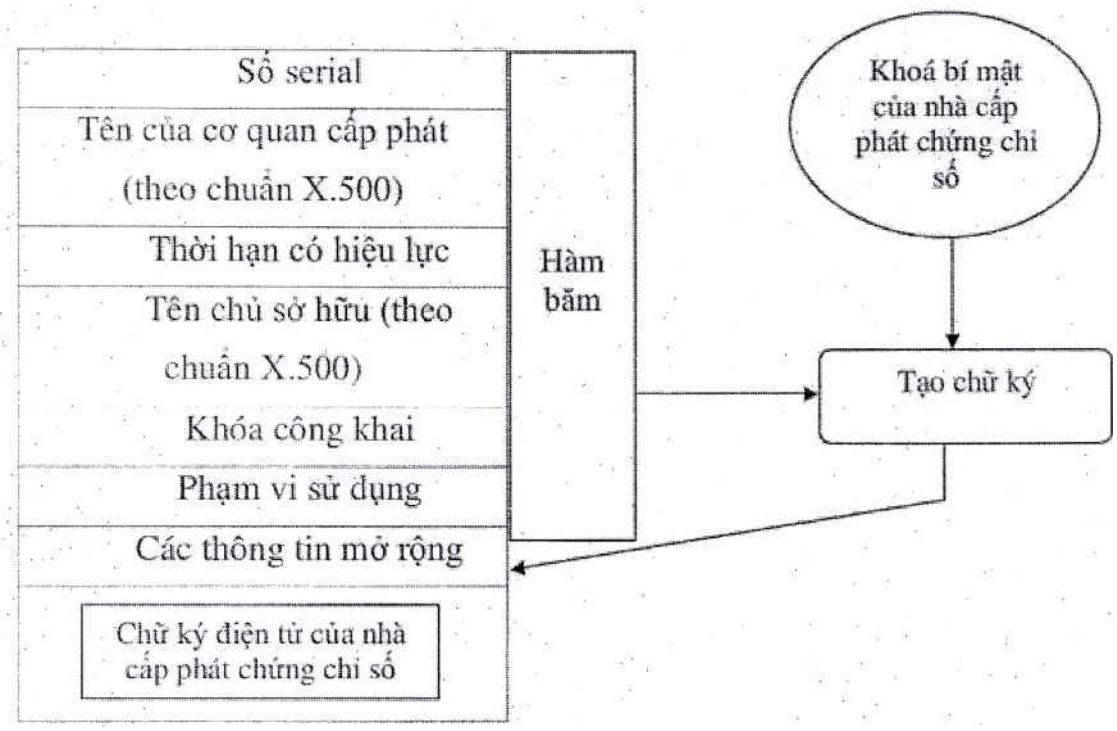
* Nhà phát hành chứng chỉ (Certi/ficate Authrity).

Thành phần này thực hiện các chức năng chính của hệ thống như:

- Tạo chứng chỉ số cho người dùng (xác thực cho các khóa công khai).

- Bảo trì cơ sở dữ liệu hệ thống, cho phép phục hồi các cặp khóa người dùng

- Yêu cầu hệ thống tuân thủ các thủ tục bảo mật.



Hình 3-12: Cấu trúc bên trong chia sẻ hệ thống chia sẻ

* Kho chứa chứng chỉ.

Thực hiện việc lưu trữ để phân phối chứng chỉ số của người dùng hệ thống CA, gồm các thông tin sau:

- Chứng chỉ số người dùng.
- Danh sách các chứng chỉ bị thu hồi.
- Thông tin chính sách người dùng.
- Cung cấp cơ chế phân phối chứng chỉ và CLRs đến các thực thể cuối.

* Cơ quan đăng ký chứng chỉ (Registration Authority).

Cung cấp giao diện cho người điều hành hệ thống thực hiện các chức năng của hệ thống CA như: Bổ sung người dùng (xác thực chứng chỉ người dùng); Quản lý người dùng và chứng chỉ của người dùng; Quản lý chính sách an toàn; Xây dựng cây xác thực.

* Mô hình tổ chức chứng thực số.

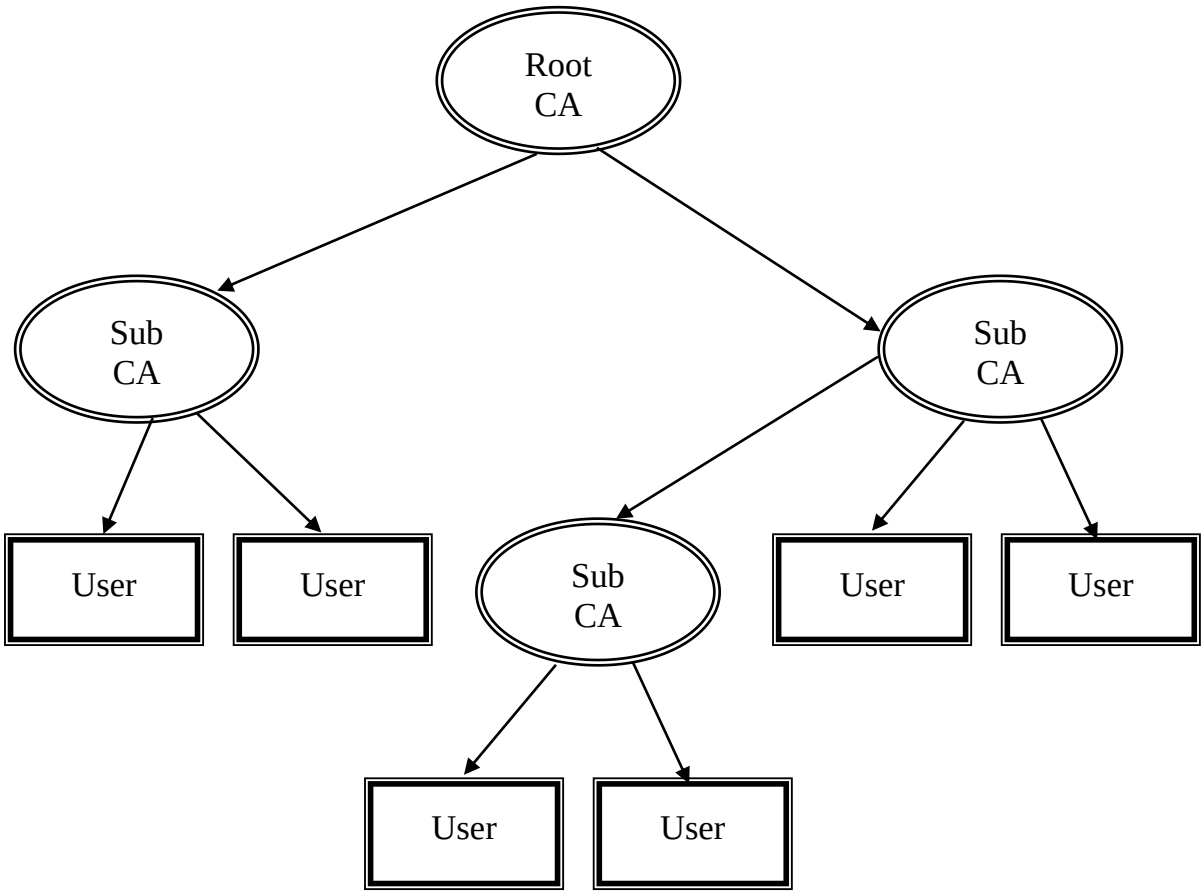
Hiện nay trên thế giới có ba mô hình tổ chức chứng thực số là:

- Mô hình phân cấp hay mô hình chứng thực gốc - Hình 3-13.

Cho phép xây dựng một hệ thống CA hình cây với một gốc duy nhất gọi là Root CA, dưới Root CA có thể là các Sub CA vả dưới Sub CA lại có thể là các Sub CA khác.

- Mô hình CA dạng lưới (Mesh CA Model) - Hình 3-14

Là một mô hình trong đó các CA ngang hàng, không phụ thuộc vào nhau, tin tưởng lẫn nhau tạo thành một mạng lưới tin tưởng qua lại với nhau.



Hình 3-12: Mô hình của Root CA

3.1.4 Phát hiện xâm nhập bằng công nghệ IDS (Intrusion Detection System). Thực tế, đây là một Hệ thống tường lửa mềm, là những phần mềm nguồn mở có sẵn trên Internet. Những phần mềm này rất thích hợp đối với các mạng riêng không lớn lắm.

Những ưu điểm của cung của chúng là:

- IDSs là những phần mềm nguồn mở nên giá thành của chúng rất rẻ.

Hiện nay BCA đã ứng dụng thành công phầm mềm SNORT để bảo vệ mạng nội bộ Ngành CA.

-Tăng khả năng phát hiện. Nếu khai thác tốt, một IDS có thể thực hiện nhiều phân tích phức tạp. Ta biết rằng, kẻ tấn công mạng thường đặt mục tiêu ban đầu là tìm cách phá hỏng bản ghi kiểm tra nhằm làm tổn thương các rào chắn của Hệ thống. Nhưng IDSs không cần dựa vào các bản ghi nhật ký này.

- Khả năng ngăn chặn từ xa. IDSs có khả năng phát hiện các dấu hiệu bị xâm nhập vào mạng dùng riêng từ xa rồi báo cho các Quản trị mạng để có biện pháp đối phó một cách chủ động.

- Về pháp lý. Một vài IDS (chẳng hạn như SNORT) gắn liền với khả năng pháp lý. Chúng có khả năng liên quan đến việc đưa ra chứng cứ thích đáng làm chứng cứ tại Toàn án khi cần. Mục tiêu chính của IDSs là cung cấp các khả năng pháp lý là thu thập và bảo quản chứng cứ về tội phạm.

- Phát hiện các hỏng hóc và khôi phục. Việc triển khai IDSs tốt có khả năng cảnh báo với các Nhà Quản trị mạng về nguy cơ Hệ thống có dấu hiệu bị hỏng.

Những nhược điểm:

- Cảnh báo sai. Phần lớn các IDSs nhiều lúc phát hiện sai như có trường hợp báo là có vi phạm sự an toàn của mạng nhưng thực tế thì không.

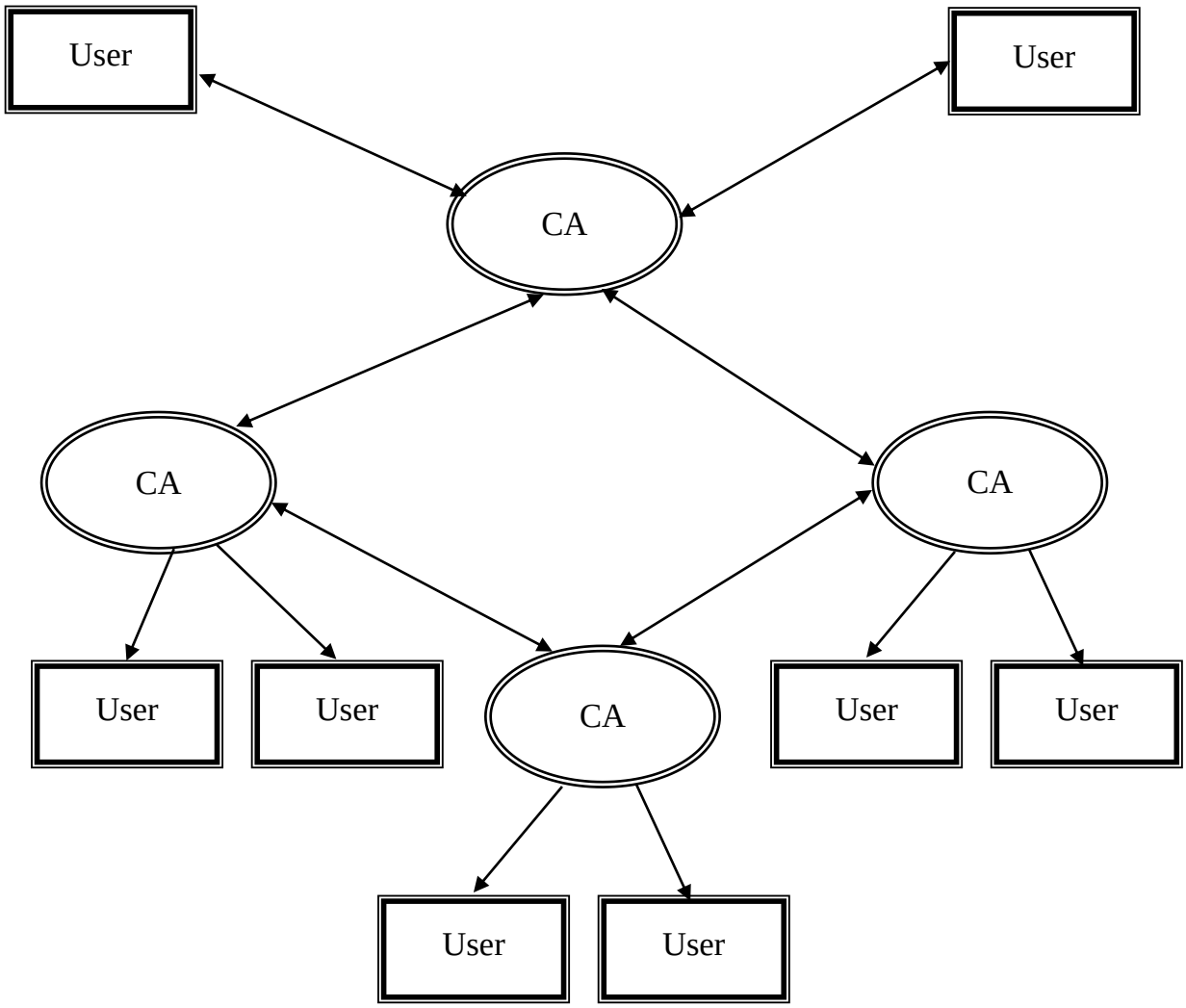
- Suy giảm hiệu suất. Việc triển khai IDSs làm cho hiệu suất của hệ thống. Lượng suy giảm đó phụ thuộc vào từng IDS cụ thể. Theo kết quả nghiên cứu và ứng dụng của BCA, SNORT được cho là tốt nhất.

- Khả năng bị tấn công. Cũng như các firewalls,các IDSs cũng có thể bị tấn công trực diện và chính IDSs. Các kẻ tấn công có thể làm ngập hệ thống làm cho chúng trở nên vô dụng trước các tấn công

.- Dễ bị giả mạo. Theo [15], có nhiều cách để có thể đánh bại các IDSs

- Thay đổi công nghệ. Vì IDSs. Việc phụ thuộc vào công nghệ cụ thể

có thể làm giảm khả khả năng phát hiện của IDSs mỗi khi toàn bộ hạ tầng mạng bị thay đổi.



Hình 3-14: Mô hình Mesh CA

- Mô hình CA cầu nối (Bridge Certification Authority CA Model).

Là một biến thể của mô hình CA dạng lưới, khi số lượng các CA cần tin tưởng qua lại với nhau là quá lớn, lúc này phát sinh nhu cầu cần tìm một CA đủ tin tưởng để các CA khác cùng tin tưởng vào CA đó và các CA thể hiện qua cầu nối trung gian.

3.1.3.2. Nguyên lý mã hóa.

Khi hai bên trao đổi thông tin phải biết khóa công khai (e_k) của nhau.

Việc biết khóa công khai (e_k) không cho phép tính ra được khóa riêng (d_k). Như vậy trong hệ thống mỗi cá thể k khi đăng ký vào hệ thống được cấp 1 cặp khóa (e_k, d_k). Trong đó e_k là chìa khóa lập mã, d_k là chìa khóa giải mã.

3.1.3.3 Nguyên lý mã hóa.

* Thuật toán Hàm băm

a. Hàm băm.

Là hàm sinh ra các giá trị băm tương ứng với các khối dữ liệu. Giá trị băm đóng vai trò như một khóa để phân biệt các khối dữ liệu, tuy nhiên người ta chấp nhận hiện tượng trùng khóa hay còn gọi là đụng độ và cố gắng cải thiện giải thuật để giảm thiểu đụng độ đó. Hàm băm thường được dùng trong bảng băm nhằm giảm chi phí tính toán khi tìm một khối dữ liệu trong một tập hợp.

b. Đảm bảo tính nguyên vẹn dữ liệu.

Hàm băm mật mã học là hàm băm và có tính chất là hàm một chiều. Từ khối dữ liệu hay hàm băm đầu vào chỉ có thể đưa ra một giá trị băm duy nhất. Đối với tính chất của hàm một chiều. Một người nào đó dù có bắt được giá trị băm, cũng không thể suy ngược lại giá trị, đoạn tin nhắn băm khởi điểm.

c. Một số hàm băm thông dụng

- Hàm băm MD5 (Hình 3-15).

Thuật toán hàm băm MD5: Được dùng trong nhiều ứng dụng bảo mật và phổ biến để kiểm tra tính toàn vẹn của tập tin, có ưu điểm tốc độ xử lý rất nhanh, thích hợp với các thông điệp dài và cho giá trị băm dài 128 bit.

- Chuẩn băm an toàn SHS.

SHS (Security Hash Standard) là chuẩn gồm các tập hợp các thuật toán băm mật mã an toàn (Security Hash Algorithm - SHA) như SHA-1, SHA-224, SHA- 256, SHA-384, SHA-512 dựa trên phương pháp của MD4 và MD5.

Thuật toán	Kích thước tính theo bit					Số chu kỳ	Các thao tác	Đụng độ	Độ an toàn
	Kết quả	Trạng thái	Khối	Thông điệp tối đa	Từ				
SHA-0	160	160	512	2^{64}-1	32	80	+, and, or, xor, rotl	Có	80
SHA-1	160	160	512	2^{64}-1	32	80	+, and, or, xor, rotl	2^{63} thao tác	80
SHA-256/224	256/224	256	512	2^{64}-1	32	64	+, and, or, xor, shr, rotl	Chưa	112/128
SHA 512/384	512/384	512	1024	2^{128}-1	64	80	+, and, or, xor, shr, rotl	Chưa	192/256

Hình 3-15: Chuẩn MD5

*** Thuật toán RSA**

***a.* Mô tả sơ lược**

RSA là một thuật toán mã hóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

***b.* Tạo khóa**

Giả sử A và B cần trao đổi thông tin bí mật qua một kênh không an toàn. Với thuật toán RSA, đầu tiên a cần tạo cho mình một cặp khóa bao gồm khóa công khai và khóa bí mật. A gửi khóa công khai cho B, và giữ bí mật khóa cá nhân của mình.

***c.* Mã hóa.**

Giả sử B muốn gửi đoạn thông tin *M* cho A. Đầu tiên B chuyển *M* thành một số *m*<*n* theo một hàm có thể đảo ngược (từ *m* có thể xác định lại được *M)* được thỏa thuận trước.

***d.* Giải mã.**

A nhận được *c từ B* và biết khóa bí mật *d.* A có thể tìm được *m* từ *c* theo công thức $m = c^d \bmod n$

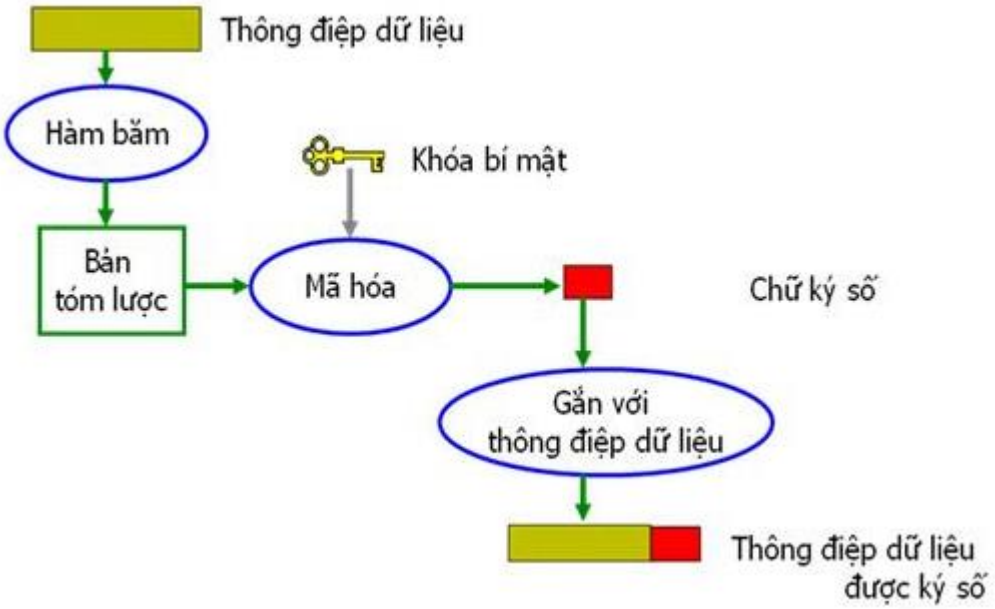
*** Thuật toán SHA**

Là thuật toán được xây dựng dựa trên MD4. Thuật toán SHA-1 tạo ra chuỗi mã băm có chiều dài cố định 160 bit, từ chuỗi bit dữ liệu đầu vào X có chiều dài tùy ý.

3.1.3.4 Chữ ký số và quản lý khóa.

* Chữ ký số (Hình 3-16)

Chữ ký số là thông tin được mã hóa bằng khóa riêng của người gửi được đính kèm theo văn bản đảm bảo cho người nhận xác thực đúng nguồn gốc, tính toàn vẹn của dữ liệu.



Hình 3-16: Quy trình ký và thẩm tra chữ ký số

**** Sử dụng chữ kỹ số như thế nào.***

Chữ ký số chỉ dùng được trong môi trường số, giao dịch điện tử với máy tính và mạng internet; Chữ ký số có thể sử dụng trong các giao dịch thư điện tử, mua bán hàng trực tuyến, đầu tư chứng khoán trực tuyến, chuyển tiền ngân hàng, thanh toán trực tuyến....

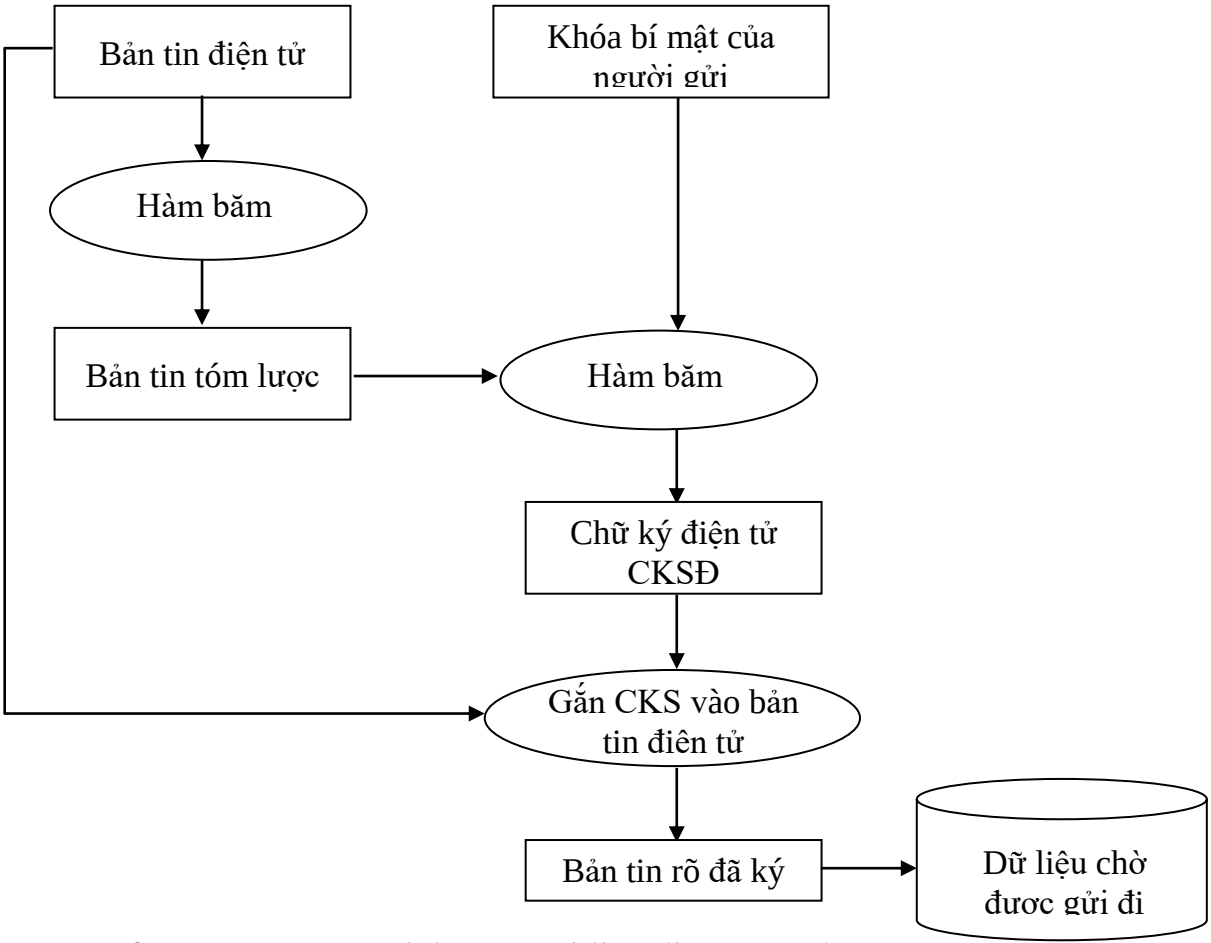
* Quy trình sử dụng chữ ký số

Ký gửi chữ ký điện tử (mã hóa)

Khi muốn gửi một văn bản quan trọng, đòi hỏi văn bản phải được ký xác nhận chính danh từ người gửi văn bản, người gửi văn bản sẽ thực hiện việc ký chữ ký điện tử.

b.Xác thực chữ ký điện tử (giải mã).

Sau khi nhận được một văn bản có đính kèm chữ ký của người gửi, người nhận phải giải mã trở lại văn bản trên và kiểm tra xem văn bản này có bị thay đổi bởi bên thứ ba hay không và chữ ký đính kèm trên văn bản có đúng của người gửi hay không.



Hình 3-17: Quả trình ký vào tài liệu điện tử sử dụng Private Key

c. Sơ đồ chữ kỷ sỗ.

Sơ đồ chữ ký là một băm (P, Ạ, K, s, V), trong đó:

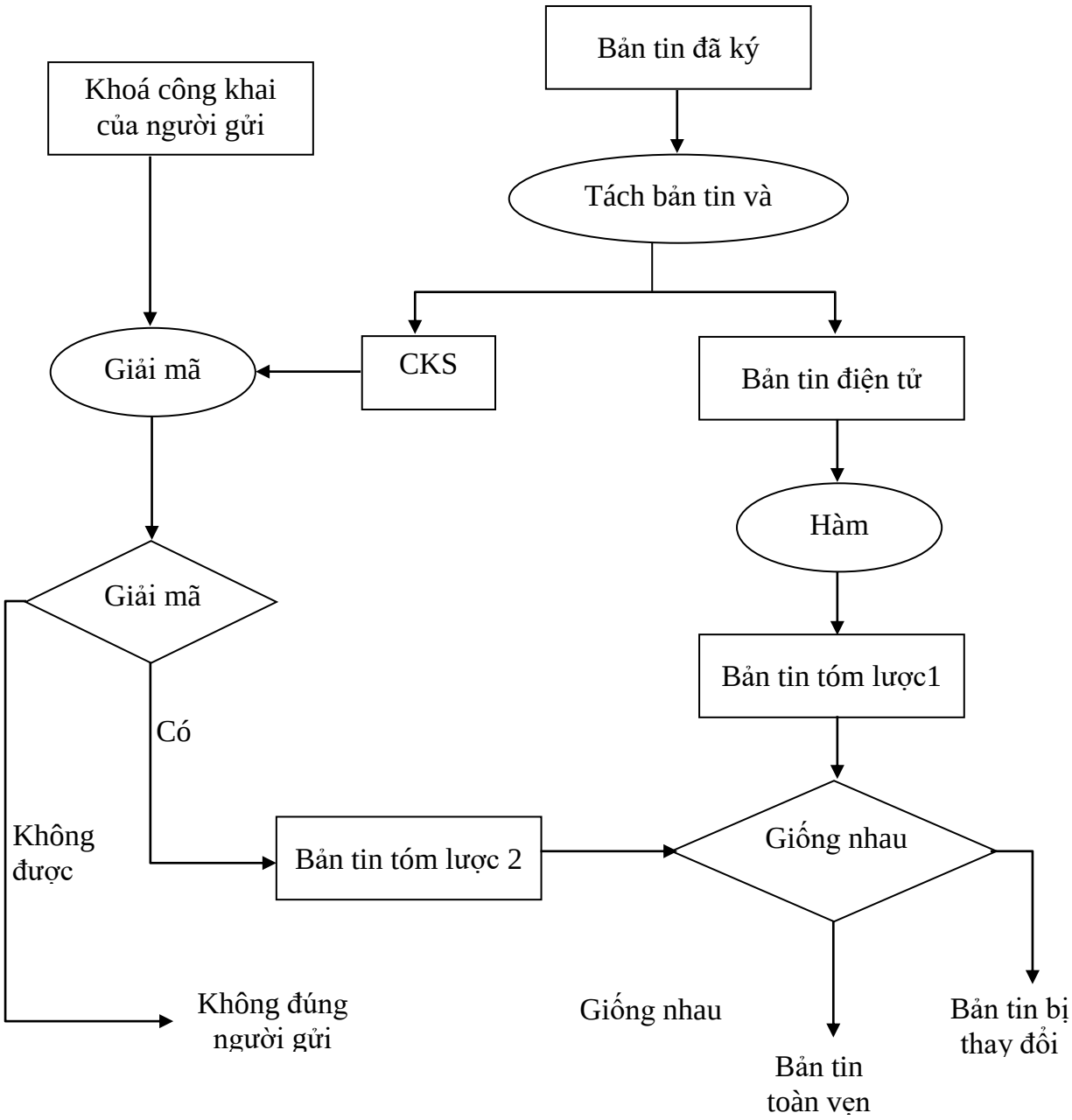
- P: là tập hợp hữu hạn các văn bản có thể.
- A: là tập hợp hữu hạn các chữ ký có thể
- K: là tập hợp hữu hạn các khóa có thể.
- S: là tập hợp các thuật toán ký.
- V: là tập họp các thuật toán kiểm thử.

d. Phân loại chữ ký số.

- Phân loại chữ ký theo đặc trung kiểm tra chữ ký.
- Phân loại chữ ký theo mức an toàn.
- Phân loại theo ứng dụng đặc trưng.

e. Quản lý khóa

Quản lý khóa là vấn đề cần quan tâm để đảm bảo an toàn cho hệ mã hóa. Đối tượng thám mã thuờng tấn công cả hai hệ mã hóa đối xứng và công khai thông qua hệ quản lý khóa.



Hình 3-18: Quản lý khóa sử dụng Private Key

3.2. Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS).

3.2.1. Khái niệm. Phát hiện xâm nhập bằng công nghệ IDS (Intrusion Detection System).

Những ưu điểm của cung của chúng là:

- IDSs là những phần mềm nguồn mở (tầng hosts) nên giá thành của chúng rất rẻ. Hiện nay BCA đã ứng dụng thành công phầm mềm SNORT để

bảo vệ mạng nội bộ Ngành CA.

-Tăng khả năng phát hiện. Nếu khai thác tốt, một IDS có thể thực hiện nhiều phân tích phức tạp. Ta biết rằng, kẻ tấn công mạng thường đặt mục tiêu ban đầu là tìm cách phá hỏng bản ghi kiểm tra nhằm làm tổn thương các rào chắn của Hệ thống. Nhưng IDSs không cần dựa vào các bản ghi nhật ký này.

- Khả năng ngăn chặn từ xa. IDSs có khả năng phát hiện các dấu hiệu bị xâm nhập vào mạng dùng riêng từ xa rồi báo cho các Quản trị mạng để có biện pháp đối phó một cách chủ động.

- Về pháp lý. Một vài IDS (chẳng hạn như SNORT) gắn liền với khả năng pháp lý. Chúng có khả năng liên quan đến việc đưa ra chứng cứ thích đáng làm chứng cứ tại Toàn án khi cần. Mục tiêu chính của IDSs là cung cấp các khả năng pháp lý là thu thập và bảo quản chứng cứ về tội phạm.

- Phát hiện các hỏng hóc và khôi phục. Việc triển khai IDSs tốt có khả năng cảnh báo với các Nhà Quản trị mạng về nguy cơ Hệ thống có dấu hiệu bị hỏng.

Nhược điểm:

- Cảnh báo sai. Phần lớn các IDSs nhiều lúc phát hiện sai như có trường hợp báo là có vi phạm sự an toàn của mạng nhưng thực tế thì không.

- Suy giảm hiệu suất. Việc triển khai IDSs làm cho hiệu suất của hệ thống. Lượng suy giảm đó phụ thuộc vào từng IDS cụ thể. Theo kết quả nghiên cứu và ứng dụng của BCA, SNORT được cho là tốt nhất.

- Khả năng bị tấn công. Cũng như các firewalls,các IDSs cũng có thể bị tấn công trực diện và chính IDSs. Các kẻ tấn công có thể làm ngập hệ thống làm cho chúng trở nên vô dụng trước các tấn công

.- Dễ bị giả mạo. Theo [15], có nhiều cách để có thể đánh bại các IDSs

- Thay đổi công nghệ. Vì IDSs. Việc phụ thuộc vào công nghệ cụ thể có thể làm giảm khả khả năng phát hiện của IDSs mỗi khi toàn bộ hạ tầng mạng bị thay đổi

Hệ thống phát hiện xâm nhập (Intrustion Detection System - IDS) là hệ thống phần cứng hoặc phần mềm có chức năng giám sát lưu thông thông mạng, tự động theo dõi các sự kiện xảy ra trên hệ thống máy tính, phân tích để phát hiện ra các vấn đề liên quan đến an ninh, bảo mật và đưa ra cảnh bảo cho nhà quản trị.

3.2.2. Các thành phần và chức năng của IDS.

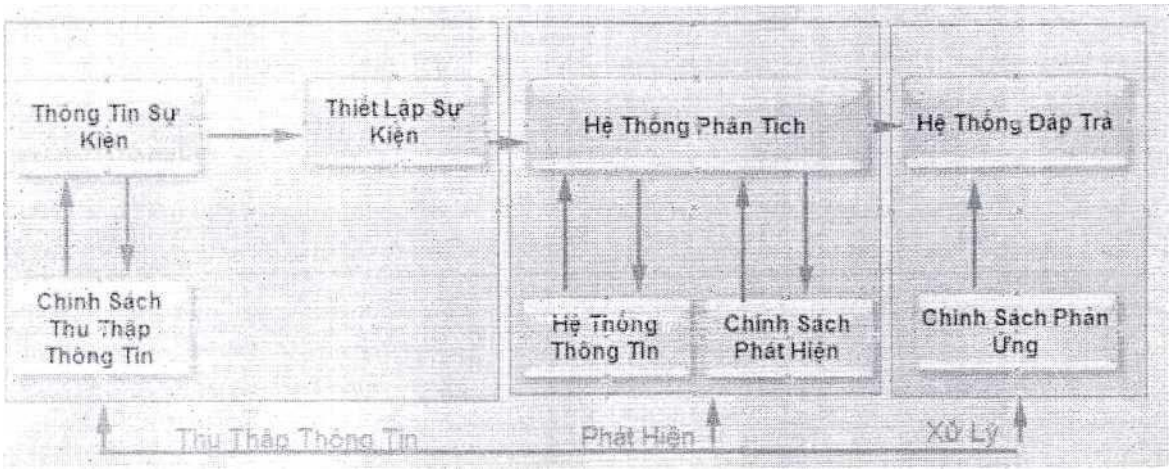
IDS bao gồm các thành phần chính

- Thành phần thu thập thông tin

gói tin. - Thành phần phát hiện

gói tin.

- Thành phần xử lý (phản hồi)



Hình 3-19 Mô hình kiến trúc phát hiện xâm nhập IDS

* ***Thành phần thu thập gói tin.***

Thành phần này có nhiệm vụ lấy tất cả các gói tin đi đến mạng. Thông thường các gói tin có địa chỉ không phải của một card mạng thì sẽ bị card mạng đó hủy bỏ nhưng card mạng của IDS được đặt ở chế độ thu nhận tất cả. Tất cả các gói tin qua chúng đều được sao chụp, xử lý, phân tích đến từng

trường thông tin. Bộ phận thu thập gói tin sẽ đọc thông tin từng trường trong gói tin, xác định chúng thuộc kiểu gói tin nào dịch vụ gì... Các thông tin này sẽ dược chuyển đến thành phần phát hiện tấn công.

***** Thành phần phát hiện gói tin.

Ở thành phần này, các bộ cảm biến đóng vai trò quyết định. Vai trò của bộ cảm biên là dùng để lọc thông tin và loại bỏ những thông tin dữ liệu không tương thích đạt được từ các sự kiện liên quan đến hệ thống bảo vệ, vì vậy có thể phát hiện được các hành động đáng ngờ

* Thành phần phản hồi.

Khi có dấu hiệu của việc tấn công hay xâm nhập, thành phần phát hiện tấn công sẽ gửi tín hiệu báo hiệu (alert) có sự tấn công hoặc xâm nhập đến thành phần phản ứng. Lúc đó thành phân phản ứng sẽ kích hoạt tuờng lửa thực hiện ngăn chặn cuộc tân công hay cảnh báo tới người quản trị. Dưới đây là một số kỹ thuật ngăn chặn:

- Cảnh báo thời gian thực:

Gửi các cảnh báo thời gian thực đến người quản trị để họ nắm được chi tiết các cuộc tấn công, các đặc điểm và thông tin về chúng.

- Ghi lại vào các tập tin:

Các dữ liệu của các gói tin sẽ được lưu trữ trong hệ thống các tập tin log. Mục đích là để người quản trị có thể theo dõi các luồng thông tin và là nguồn thông tin giúp cho module phát hiện tấn công hoạt động.

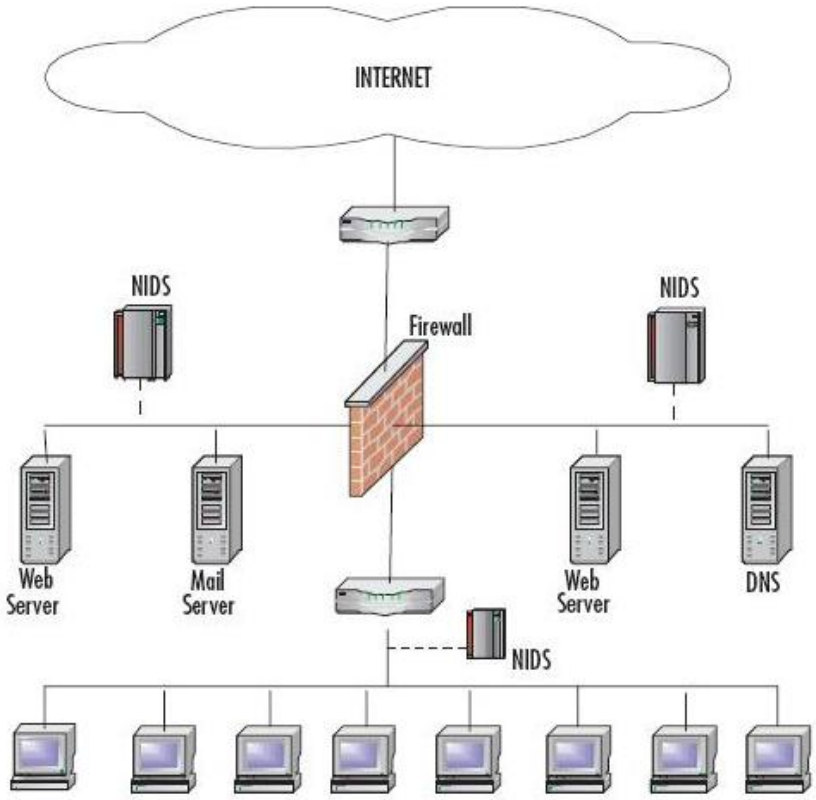
- Ngăn chặn, thay đối gói tin:

Khi một gói tin khớp với dấu hiệu tấn công thì IDS sẽ phản hồi bằng cách xóa bỏ, từ chối hay thay đổi nội dung của gói tin, làm cho gói tin trở nên không bình thường.

***** Phân loại IDS

a. Network Base IDS (NIDS)

Hệ thống IDS dựa trên mạng sử dụng nội bộ dò và cảm biến được cài đặt trên toàn mạng. Những bộ dò này theo dõi trền mạng nhàm tìm kiếm những lưu lượng trùng với những mô tả sơ lược được định nghĩa hay là những dấu hiệu.



Hình 3-20: Network base IDS

- Lợi thế của Network Base IDS:
  + Quản lý được cả một Network Segment (gồm nhiều host).
  + Cài đặt và bảo trì đơn giản, không ảnh hưởng tới mạng.
  + Tránh DOS ảnh hưởng tới một host nào đó.
  + Có khả năng xác định lỗi ở tầng netvvork (trong mô hình OSI).
  + Độc lập với hệ điều hành.
- Hạn chế của Network Base IDS:
  + Có thể xảy ra trường hợp báo động giả.

+ Không thể phân tích các gói tin đã được mã hóa (SSL, SSH, IPSec...).

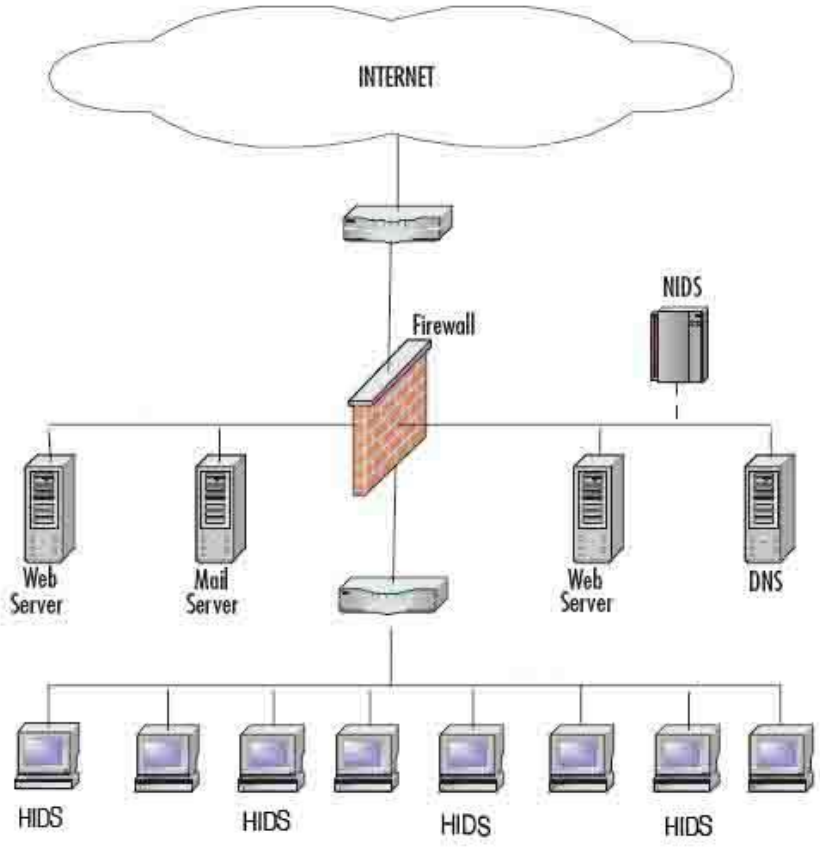
+ NIDS đòi hỏi phải được cập nhật các signature mới nhất để thực sự an toàn

+ Có độ trễ giữa thời điểm bị tấn công với thời điểm báo động. Khi báo động được phát hiện ra, hệ thống có thể đã bị tổn hại.

+ Không cho biết việc tấn công có thành công hay không.

b. HostBaselDS (HIDS).

HIDS thường cài đặt trên một máy tính nhất định. Thay vì giám sát hoạt động của một network segment, HIDS chỉ giám sát các hoạt động trên một máy tính



Hình 3-20: Host base IDS

- Lợi thế của Host Base IDS:

+ Có khả năng xác định người dùng liên quan tới một sự kiện.

+ HIDS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy.

+ Có thể phân tích các dữ liệu đã hóa.

+ Cung cấp các thông tin về host trong lúc cuộc tấn công diễn ra.

- Hạn chế của Network Base IDS:

+ Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.

+ Khi hệ điều hành bị "hạ" do tấn công thì đồng thời HIDS cũng bị "hạ".

+ HIDS cần phải được thiết lập trên từng host cần giám sát.

+ Có độ trễ giữa thời điểm bị tấn công với thời điểm báo động. Khi báo động được phát hiện ra, hệ thống có thể đã bị tổn hại.

+ HIDS không có khả năng phát hiện các cuộc dò quét mạng (Nmap, Netcat...).

+ HIDS cần tài nguyên trên host để hoạt động.

+ HIDS có thể không hiệu quả khi bị DOS.

+ Đa số chạy trên hệ điều hành Window. Tuy nhiên cũng có một số chạy trên UNIX và các hệ điều hành khác.

*** Cơ chế hoạt động của IBS.**

IDS có hai chức năng chính là phát hiện các cuộc tấn công và cảnh báo các cuộc tấn công đó. Có hai phương pháp khác nhau để phân tích các sự kiện để phát hiện các vụ tấn công: phát hiện dựa trên các dấu hiệu và phát hiện dựa trên sự bất thường. Các sản phẩm của IDS có thể sử dụng một trong hai cách hoặc sử dụng kết hợp cả hai.

a. Phát hiện dựa trên sự bất thường.

Công cụ này thiết lập một hiện trạng các hoạt động bình thường và sau đó duy trì một hiện trạng hiện hành cho một hệ thống. Khi hai yếu tố này xuất

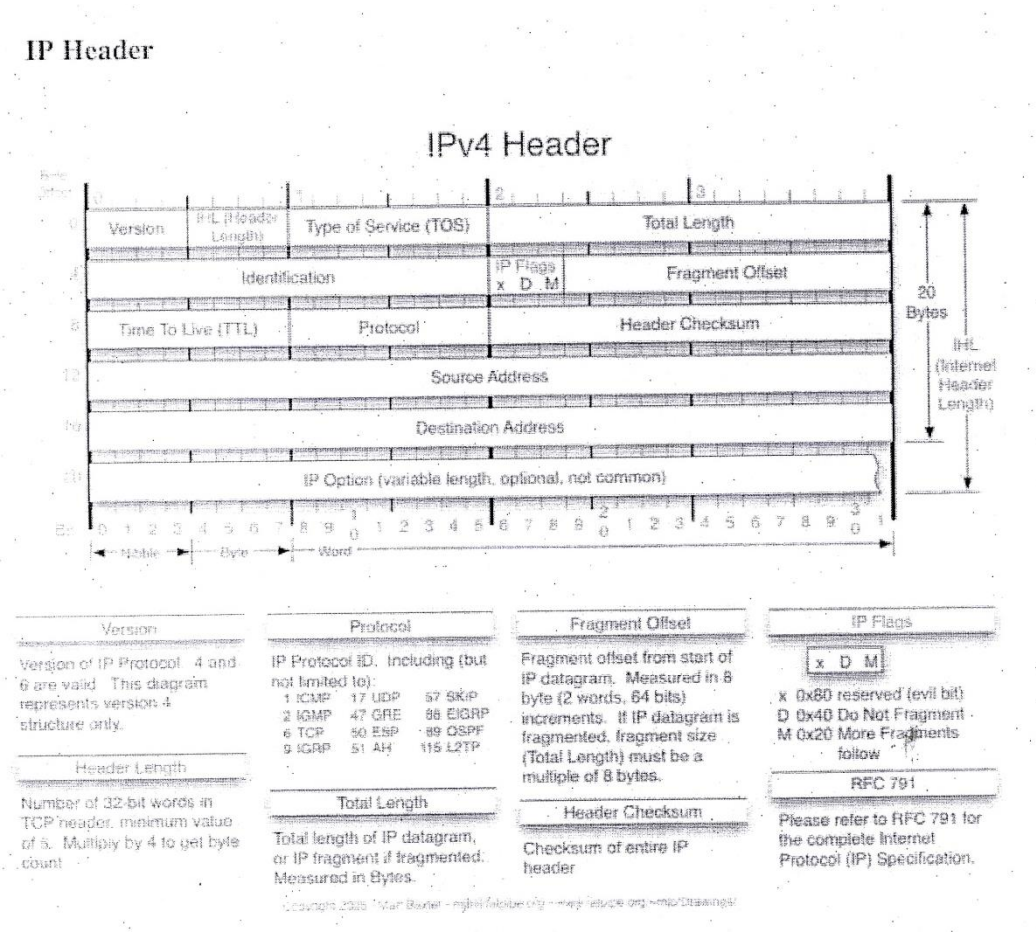
hiện sự khác biệt, nghĩa là đã có sự xâm nhập.

Ví dụ: Một địa chỉ IP của máy tính A thông thường truy cập vào domain của công ty trong giờ hành chính, việc truy cập vào domain của công ty ngoài giờ làm việc là một điều bất thường.

b. Phát hiện thông qua Protocol.

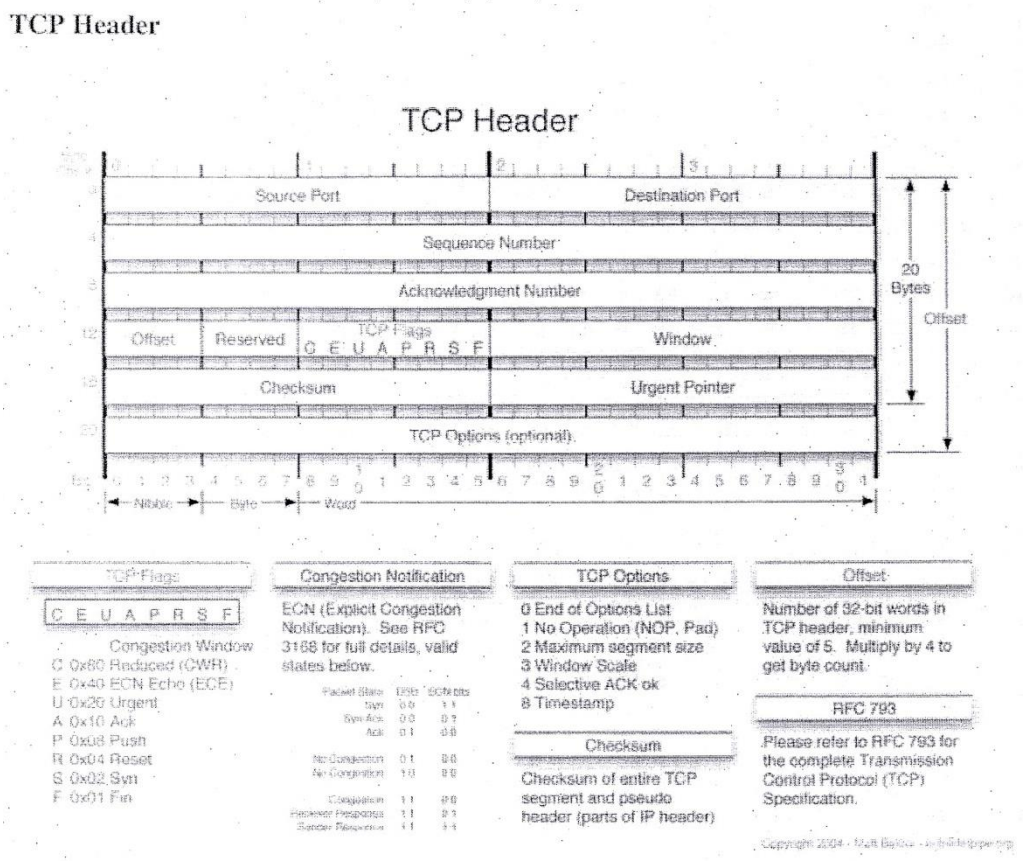
Tương tự như việc phát hiện dựa trên dấu hiệu, nhưng nó có thực hiện một sự phân tích theo chiều sâu của các giao thức được xác định cụ thể trong gói tin.

Sau đây là câu trúc của một gói tin



Hình 3-20: cấu trúc TCP Header

Thuộc tính Source Address và Destination Address giúp cho IDS biết được nguồn gốc của cuộc tấn công.



Hình 3-20: cấu trúc TCP Header

Các hệ thống IDS khác nhau đều dựa vào phát hiện các xâm nhập trái phép và những hành động dị thường. Quá trình phát hiện có thể được mô tả bởi 3 yếu tố cơ bản nền tảng, như sau:

-*Thu thập thông tin:* Kiểm tra tất cả các gói tin trên mạng.

-*Sự phân tích:* Phân tích tất cả các gói tin đã thu thập để cho biết hành động nào là tấn công.

-*Cảnh báo:* Hành động cảnh báo cho sự tấn công được phân tích ở trên.

c.Phát hiện nhờ quá trình tự học.

Kỹ thuật này bao gồm hai bước: Khi bắt đầu thiết lập, hệ thống phát hiện tấn công sẽ chạy ở chế độ tự học và tạo ra một hồ sơ về cách cư xử của

mạng với các hoạt động bình thường. Sau thời gian khởi tạo, hệ thống sẽ chạy ở chế độ làm việc, tiến hành theo dõi phát hiện các hoạt động bất thưởng của mạng bằng cách so sánh với hồ sơ đã thiết lập. Chế độ tự học có thể chạy song song với chế độ làm việc để cập nhật hồ sơ của mình nhưng nếu dò ra có tín hiệu tấn công thì chế độ tự học phải dừng lại cho tới khi cuộc tấn công kết thúc.

* Các ứng dụng IDS phổ biến hiện nay.

Trong hoàn cảnh hiện nay, với tần suất tấn công và xâm nhập ngày càng phổ biến thì khi một tổ chức kết nối với internet không thể áp dụng các phương pháp phòng chống tấn công, xâm nhập sử dụng firewall chỉ là một trong các biện pháp căn bản, sơ khai trong công tác phòng chống xâm phạm thông tin. Sử dụng IDS sẽ góp phần tăng cường sức mạnh cho nhà quản trị và cảnh báo kịp thời mọi thời điểm diễn biến thất thường qua mạng. Cụ thể, IDS có thể cảnh báo những hành động sau:

- Hành động download dữ liệu trong hệ thống LAN bằng ftp từ các máy ip lạ.
- Hành động chat với các máy ip lạ.
- Hành động cố tình truy xuất những website bị công ty cấm truy cập.
- Hành động truy xuất các website vào giờ cấm.
- Hành động chống sniff sử dụng phương pháp ARP SpooTmg.
- Thực hiện chống Dos vào server thông qua lỗi tràn bộ đệm.

3.2.3. Bảo mật Web.

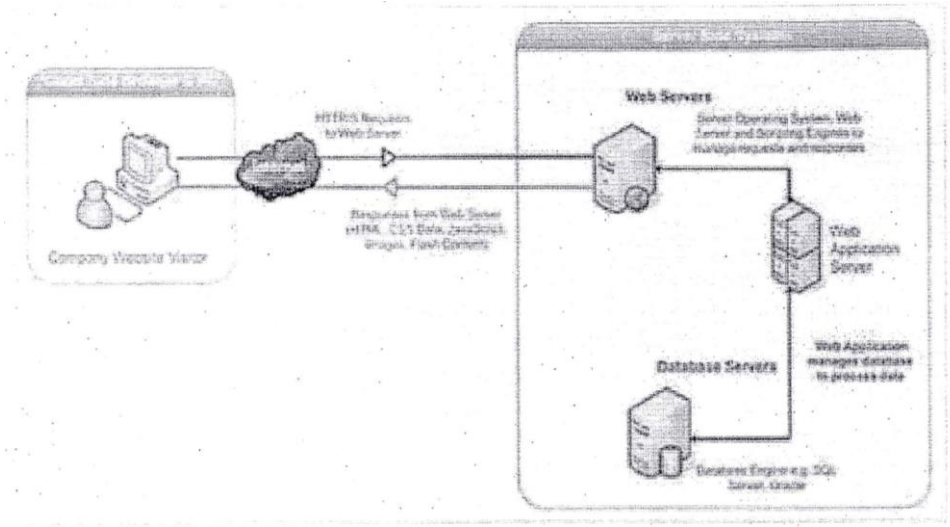
* Tìm hiểu ứng dụng web

* Ủng dụng web là gì.

Ứng dụng web là một trình ứng dụng mà có thể tiếp cập qua web thông qua mạng internet hay intranet. Ứng dụng web được dùng để bán hàng trực tuyến, diễn đàn thảo luận, Weblog và nhiều chức năng khác.

Cấu trúc mật ứng dụng web (Hình 3-21)

Ứng dụng web được cấu trúc như một ứng dụng ba lớp. Thứ nhất là trình duyệt web, lớp giữa sử dụng công nghệ web động, lớp thứ ba là cơ sở dữ liệu. Trình duyệt sẽ gửi dữ liệu đến lớp giữa để tạo ra truy vấn, cập nhật CSDL và tạo ra giao diện người dùng.



Hình 3-21: Mô hình quá trình duyệt Web

* ***Domain - Hosting***

Mạng internet là mạng máy tính toàn cầu, nên internet có cấu trúc địa chỉ, cách đánh địa chỉ đặc biệt, khác cách tổ chức địa chỉ của mạng viễn thông. Khi sử dụng internet, người dùng không cần biết hoặc nhớ đến địa chỉ IP mà chỉ cần nhớ tên miền là truy cập được.

a. Cấu tạo của tên miền:

Gồm nhiều thành phần tạo nên, cách nhau bởi dấu chấm. Thành phần thứ nhất "home" là tên của máy chủ, thành phần thứ hai "vnn" thường gọi là tên miền mức hai, thành phần cuối cùng "vn" là tên miền mức cao nhất.

b. Tên miền mức cao nhất (Top Level Domain - TLD):

Bao gồm các mã quốc gia của các nước tham gia internet được quy định bằng chữ cái theo tiêu chuẩn ISO - 3166.

c. Tên miền mức hai (Second Level)

Tên miền mức hai này là do tổ chức quản lý mạng của mỗi quốc gia định nghĩa theo các lĩnh vực kinh tế, chính trị, xã hội...

d. Các loại tên miền:

- Tên miền cao cấp nhất là tên miền trực tiếp đăng ký với các nhà cung cấp tên miền.

- Tên miền thứ cấp: Là tất cả những loại tên miền còn lại mà tên miền đó phải phụ thuộc vào một tên miền cao cấp nhất. Để đăng ký các tên miền kiểu này, thông thường phải liên hệ trực tiếp với người quản lý tên miền cấp cao nhất.

- Web hosting: Web hosting là nơi luu trữ tất cả trang web, các thông tin của website trên một máy chủ internet.

Các yêu cầu và tính năng của Web hosting:

- Web hosting phải có một dung lượng lớn để lưu trữ thông tin của website.

- Phải hỗ trợ truy xuất máy chủ bằng giao thức FTP để cập nhật thông tin website.

- Phải có băng thông đủ lớn để phục vụ trao đổi thông tin website.

- Hỗ trợ các công cụ lập trình trên internet.

- Hỗ trợ các dịch vụ email như POP3 email, email forwarding...

***** Web server.

Là máy chủ có dung lượng lớn, tốc độ cao để lưu trữ thông tin và những website đã được thiết kế cùng với những thông tin liên qua khác.

3.3. Bảo mật ứng dụng web.

***** Bảo mật là gì?

Bảo mật web là yêu cầu tất yếu bởi vì những máy tính mang tính toàn cầu đang ngày trở nên kém an toàn và phải đối mặt với các nguy cơ về an ninh rất cao

- 3 yếu tố đảm bảo an ninh thông tin:

+ ***Tính bảo mật:*** đảm bảo chỉ người được phép mới có thể truy cập thông tin.

+ ***Tính toàn vẹn:*** đảm bảo chính xác và đầy đủ của thông tin và các phương pháp xử lý thông tin.

+ ***Tính sẵn sàng:*** đảm bảo người sử dụng được phép có thể truy cập thông tin.

****Các phương pháp gây mất an toàn thông tin (Hình 3-22)***

- Thu thập thông tin chung để tìm kiếm các thông tin xung quanh website.

Hình 3-22: Mô hình phương thức tấn công

-Môi trường mạng, hệ điều hành, ngôn ngữ lập trình, hệ quản trị cơ sở dữ liệu.

- Các cổng dịch vụ tương ứng đang mở trên server.

- Số lượt truy cập, băng thông của website.

- Khảo sát ứng dụng web.

- Thăm dò, phát hiện lỗi.

- Khai thác lỗi để tấn công: đây là giai đoạn quan trọng nhất để có thể

phá hoại hoặc chiếm quyền điều khiển được website.

- Một vài các thức tấn cồng phổ biến:

+ SQL Injection: là kỹ thuật tấn công cho phép kẻ tấn công lợi dụng lỗ hổng trong việc kiểm tra dữ liệu đưa vào ứng dụng web để thi hành các câu lệnh SQL bất hợp pháp.

+ Session Hijacking: là sử dụng phiên làm việc của một người dùng, đã tạo được một kết nối hợp lệ bằng một phương pháp không hợp lệ.

+ Local Attack: là kiểu tấn công nội bộ từ bên trong, đây là khái niệm xuất hiện khi các máy chủ mạnh lên trong thời gian gần đây.

*****Các phương thức gây mất cin toàn thông tin từ phía người quản trị.

Hiện nay việc xây dựng các ứng dụng trên web với mã nguồn mở phát triển rất mạnh, vì thế bất kỳ một website nào cũng có khả năng bị tấn công.

3.4. Đề xuất phương án phòng thủ và xây dựng demo

3.4.1. Đề xuất phương án phòng thủ

Một Trong những năm gần đây, Việt Nam ngày càng phát triển và nhất là về mặt công nghệ thông tin. Đặc biệt là về ứng dụng web, hầu như mỗi người ai cũng đã từng nghe và làm việc trên các ứng dụng web. Website trở nên phổ biến và trở thành một phần quan trọng của mỗi người, đặc biệt là các doanh nghiệp, tổ chức. Bên cạnh đó lý do an toàn bảo mật cho ứng dụng web luôn là một vấn đề nan giải. Một số phương án phòng thủ của website phổ biến hiện nay như:

• SQL Injection.

- Cách tấn công

Tin tặc trèn vào trang login những câu lệnh truy vấn đặc biệt nhu các ký tự *, like, %.... Mục đích là lấy cắp thông tin trong dabase nếu như lập trình viên vẫn sử dụng việc truy vấn dữ liệu ở dạng thuần SQL.

-Cách phòng thủ

Tối ưu hóa các hàm thực thi, truy vấn vào database (SQL, Oracle.....) bằng việc truy vấn thông qua các procedure, function, qua tham số.

Session Hiịacking.

- Cách tấn công

Ví dụ một người đang truy cập một website với thông tin User, password của người đó để thực hiện một số hình thức giao dịch kinh doanh qua website, khi người đó làm xong công việc và ra về. Một tin tặc nhay vào máy đó để sử dụng tiếp, và cố tình mở website vừa nãy người dùng truy cập vào. Nếu như lập trình viên tạo ra website không clear session, các giá trị trên cookie khi tắt trình duyệt hay set một khoảng thời gian time out thì tin tặc sẽ lợi dụng để lấy các thông tin còn lưu lại trên session hoặc cookie để truy cập vào website.

- Cách phòng thủ

Không để lộ thông tin nhạy cảm như User, password trong session, giá trị cookie trên browser. Khi sign out, hoặc tắt trình duyệt thì hệ thống phải tự động clear toàn bộ cookie và session.

* Cross Site Scripting (XSS)

- Cách tấn công

Tin tặc sẽ cố tình trên những đoạn lệnh trên clien, browser thông qua các file js, css... bên phía Client. Trước khi submit hành động lên server, nếu như lập trình viên xử lý chức năng không tốt thì những đoạn lệnh tin tặc thêm vào sẽ là cơ hội để lấy thông tin, phá hủy một số chức năng phía server.

- Cách phòng thủ.

Với những chức năng để cho phía Client có thể input data như textbox thì cần phải xử lý việc encode data trước khi save vào database.

3.4.2. Xây dựng mô hình demo phòng thủ

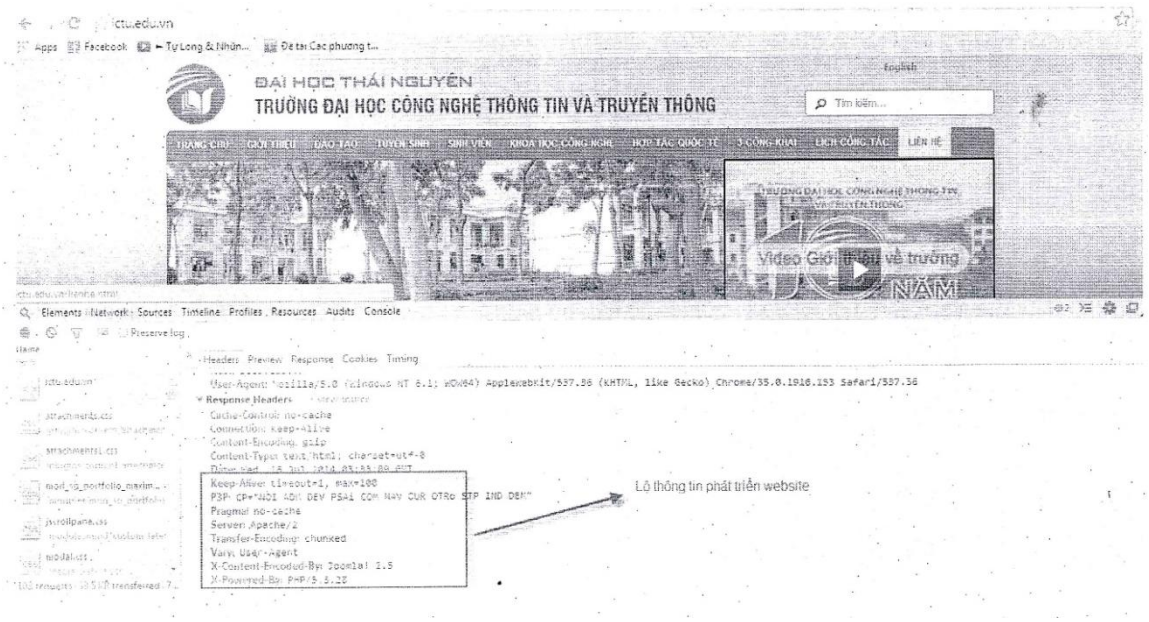
Cách đơn giản nhất để hacker hay một anonymous (nặc danh) trước khi

muốn tấn công một website là tìm ra các lỗi cơ bản thông qua mệt số tool. Một trong những tool mà nặc danh hay dùng hiện nay là chương trình Web Vulnerability Scaner để dò quét lỗi website. Sau đây sẽ demo một số phương pháp phòng thủ cơ bản của website:

Lộ thông tin về sản phẩm

Tình Trạng

-Các website trên mạng thường bị lộ các thông tin về sản phẩm để phát triển website như sofware version, từ đó làm cho hacker dễ dàng tấn công hơn, giảm thời gian truy vấn để trực tiếp tấn công thẳng vào version tương ứng của sản phẩm



Cách khắc phục

Thêm các đoạn lệnh sau vào webconfig:

<httpProtocol>

< customHeaders >

<femove name="MicrosoftSharePointTeamServices " />

<*remove name=”*X-Cotttent-Encoded-By"/>

<remove name="X-Powered-By"/>

<add name="X-Frame-Options" value="SAMEORIGIN” />

</customHeaders>

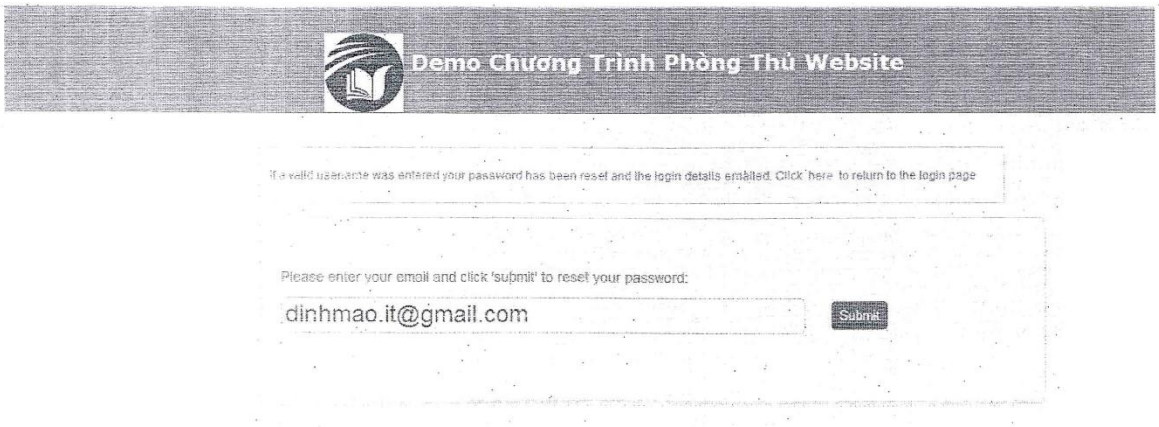
</httpProtocol>

* Lộ account khi forgot password

Tình Trạng

Các website hầu hết đều cố chức năng forgot password, khi điền một email hợp lệ, hệ thống thông báo rằng email đã hợp lệ ngay trên giao diện. Điều này vô tình làm lộ thông tin account đó có tồn tại trong hệ thống, và hacker sẽ giảm số thao tác để tìm vả tấn công vào account đó.

Cách khắc phục



Sửa lại message thông báo cho hợp lý.

Để tạo ra một sản phẩm phần mềm, một website đã khó thì bên cạnh đó việc bảo mật, tạo tính bản quen của sản phẩm cũng hết sức quan trọng. Ngoài những phương pháp cơ bản để tránh tấn công thì chúng ta cần phải update website liên tục theo định kỳ, cần phải được backup server, các dữ liệu quan trọng để tăng tính bảo mật, an toàn cao cho sản phẩm, website

3.5. Kết luận và hướng phát triển

3.5.1. Kết quả đạt được

Sau 15 tuần làm luận văn tốt nghiệp với sự hướng dẫn tận tình của thầy giáo TS. Hồ Văn Canh , luận văn tốt nghiệp của em đã được hoàn thành đúng thời hạn và đạt được những kết quả như sau:

- Trình bày tổng quan về an ninh mạng trong nước và quốc tế
- Nêu bật các lỗ hổng bảo mật của mạng máy tính và hệ điều hành
- Nêu rõ một số định nghĩa liên quan tới bảo mật, web, mạng.
- Nêu bật một số lỗi thông dụng và cách tấn công, phòng thủ trong website
- Xây dựng thành công chương trình demo về phòng thủ một số phương pháp tấn công qua vvebsite

3.5.2. Hướng phát triển

- Hiểu được các phương pháp tấn công, phòng thủ cơ bản qua mạng máy tính hay website sẽ làm cho các lập trình viên phái triển các ứng dụng với tính bảo mặt, an toàn cho sản phẩm cao hơn.

-Tấn công, phòng thủ mạng hiện tại chỉ được quan tâm với số nhiều bởi các chuyên gia, các trung tâm bảo mật, các doanh nghiệp, chính phủ. Và vì thế nó rất hữu ích và hiệu quả cao khi được đưa vào các lớp, các khóa học của sinh viên.

Em xin chân thành cảm ơn

TÀI LIỆU THAM KHẢO

[1] Bảo mật trên mạng, Bí quyết và giải pháp, NXB Thống kê, 3/2000

[2] Báo CAND số ra ngày 19/9/2016.

[3] COHE07Cohen, F., Managing network security- part 14: 50 ways to defeat Your intrusion detection system, Network Security,December 1997,pp.11-14.

[4] Dương Thanh Tuấn, Tìm hiểu kỹ thuật phòng thủ mạng, 2014.

[5] Hacking Exposed - Linux cna Brian Hatch - James Lee - George Kurtz.

[6] Hacking Exposed - Windows 2000 cna Joel Scambray - Stuart McClure.

[7] Một số hình thức tấn công mạng phổ biến, Bkav security

[8] Nguyễn Anh Tuấn, Các vấn đề về an ninh mạng, 2008 Network

[9] Security Secrets & Solution cna Joel Scambray - Stuart McClure

[10] Thái Hồng Nhị, An toàn thông tin mạng máy tính, truyền tin số và truyền dữ liệu, NXB Khoa học và kỹ thuật.

[11] Tài liệu kèm phần mềm FreeS/WAN (http:// www.freeswan.org)

[12] http://www.bkav.com.vn

[13] http://www.hackerVN.net

[14] http://packetstorm.secuify.com

[15] http://www.warez.com/archive/serialnumbers