

CHƯƠNG 1

GIỚI THIỆU

TỔNG QUAN AN NINH MẠNG

Khi hệ thống mạng được ra đời, nhu cầu cần trao đổi tài nguyên được đặt ra và những người sử dụng hệ thống mạng đó được trao đổi tài nguyên với nhau. Sau một khoảng thời gian sử dụng, hệ thống mạng ngày càng được mở rộng và số lượng người tham gia vào mạng ngày càng gia tăng, do đó việc thực hiện các chính sách bảo mật, thiết lập các chính sách trong việc truy xuất tài nguyên mạng được đặt ra. Thuật ngữ AAA ra đời.

AAA được viết tắt từ: Access Control, Authentication và Auditing

AAA là một qui trình được dùng để bảo vệ dữ liệu, thiết bị và bảo đảm tính bí mật của thông tin.

AAA là khái niệm cơ bản của an ninh máy tính và an ninh mạng. Những khái niệm này được dùng để bảo đảm các tính năng bảo mật thông tin, toàn vẹn dữ liệu và tính sẵn sàng của hệ thống.

I. ĐIỀU KHIỂN TRUY CẬP

Là một chính sách, phần mềm hay phần cứng được dùng để cho phép hay từ chối truy cập đến tài nguyên.

Qui định mức độ truy xuất đến tài nguyên.

Có 3 mô hình được sử dụng để giải thích cho mô hình điều khiển truy cập:

- MAC (Mandatory Access Control)
- DAC (Discretionary Access Control)
- RBAC (Role-based access control)

MAC (Mandatory Access Control)

Mô hình MAC làm một mô hình tĩnh được sử dụng để định nghĩa trước những quyền hạn truy cập files trên hệ thống. Người quản trị hệ thống thiết lập các quyền hạn này và kết hợp chúng với tài khoản, tập tin, tài nguyên. Mô hình MAC rất hạn chế. Trong mô hình MAC này, người quản trị là người thiết lập quyền truy cập, người quản trị cũng chỉ là

người có thể thay đổi quyền truy cập. Người dùng không thể tự thay đổi quyền chia sẻ tài nguyên của mình khi mối quan hệ tính (quyền hạn được xây dựng tĩnh) này vẫn còn tồn tại.

Ví dụ:

Quyền tập tin, thư mục trên windows 2000 (Full control, Write, Read, List folder content...)

DAC (Discretionary Access Control)

Là tập các quyền hạn truy cập trên một đối tượng mà một người dùng hay một ứng dụng định nghĩa. Mô hình DAC cho phép người dùng chia sẻ tập tin và sử dụng tập tin do người khác chia sẻ. Mô hình DAC thiết lập một ACL (Access Control List) dùng để nhận ra người dùng nào được quyền truy cập đến tài nguyên nào. Điều này cho phép người dùng gán hay loại bỏ quyền truy cập đến mỗi cá nhân hay nhóm dựa trên từng trường hợp cụ thể.

Người sở hữu có thể cung cấp quyền điều khiển cho người khác.

RBAC (Role-based access control)

Quyền hạn dựa trên công việc và phân nhóm người dùng

Khả năng cho phép cấu hình phức tạp

II. XÁC THỰC

Quá trình dùng để xác nhận một máy tính hay một người dùng cố gắng truy cập đến tài nguyên.

Ngoài ra quá trình này còn có thể sử dụng các công nghệ tiên tiến như thẻ thông minh, thiết bị sinh học, hay các phần cứng điều khiển truy cập mạng như Routers, remote access...

Username/Password

Đây là phương pháp xác nhận cổ điển và được sử dụng rất phổ biến (do tính năng đơn giản và dễ quản lý)

Mỗi người dùng sẽ được xác nhận bằng một tên truy cập và mật khẩu.

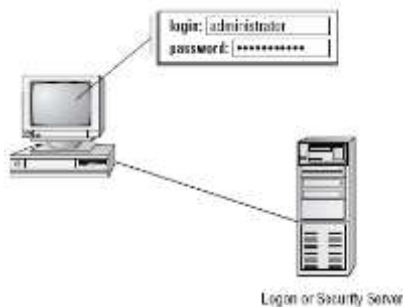
Mật khẩu thông thường được lưu dưới dạng mã hóa

Mật khẩu dễ dàng bị đoán bằng các phương pháp vét cạn

Chính sách mật khẩu:

- Mức độ không an toàn: ít hơn 6 ký tự

- Mức độ an toàn trung bình: 8 đến 13 ký tự
- Mức độ an toàn cao: 14 ký tự
- Ngoài ra mật khẩu cần tuân theo một số yêu cầu sau:
- Kết hợp giữa các ký tự hoa và thường
- Sử dụng số, ký tự đặc biệt, không sử dụng các từ có trong từ điển
- Không sử dụng các thông tin cá nhân để đặt mật khẩu (ngày sinh, số điện thoại, tên người thân...)



Kerberos

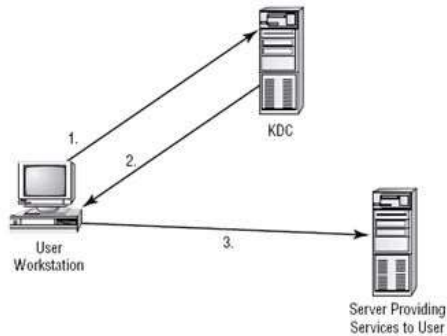
Kerberos là một dịch vụ xác nhận bảo đảm các tính năng an toàn, xác nhận một lần, xác nhận lẫn nhau, và dựa vào thành phần tin cậy thứ 3.

An toàn: sử dụng ticket, dạng thông điệp mã hóa có thời gian, để chứng minh sự hợp lệ của người dùng. Vì thế mật khẩu của người dùng có thể được bảo vệ tốt do không cần gửi qua mạng hay lưu trên bộ nhớ máy tính cục bộ.

Xác nhận truy cập 1 lần: người dùng chỉ cần đăng nhập 1 lần và có thể truy cập đến tất cả các tài nguyên trên một hệ thống hay máy chủ khác hỗ trợ nghi thức Kerberos.

Thành phần tin cậy thứ 3: làm việc thông qua một máy chủ xác nhận trung tâm mà tất cả các hệ thống trong mạng tin cậy.

Xác nhận lẫn nhau: không chỉ xác nhận người dùng đối với hệ thống mà còn xác nhận sự hợp lệ của hệ thống đối với người dùng.



Mô hình xử lý chứng thực bằng Kerberos
KDC - Key Distribution Center

CHAP

Đây là nghi thức xác nhận truy cập từ xa mà không cần gửi mật khẩu qua mạng.

Chap thường được dùng để bảo vệ các thông tin xác nhận và kiểm tra kết nối đến tài nguyên hợp lệ

Sử dụng một dãy các thách thức và trả lời được mã hóa

Chap được sử dụng để xác định sự hợp lệ bằng cách sử dụng cơ chế bắt tay 3-way. Cơ chế này được sử dụng khi kết nối được khởi tạo và được sử dụng nhiều lần để duy trì kết nối.

Nơi cần xác nhận sẽ gửi một thông điệp “challenge”

Bên nhận sẽ sử dụng một hàm băm 1 chiều để tính ra kết quả và trả lời cho bên cần xác nhận

Bên cần xác nhận sẽ tính toán hàm băm tương ứng và đối chiếu với giá trị trả về. Nếu giá trị là đúng thì việc xác nhận hợp lệ, ngược lại kết nối sẽ kết thúc.

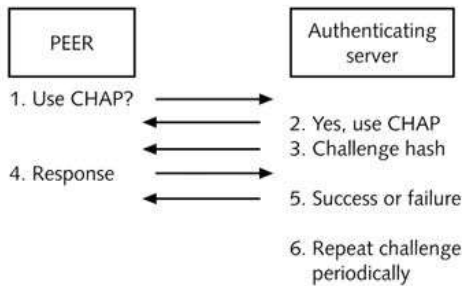


Figure 2-4 CHAP challenge-and-response process

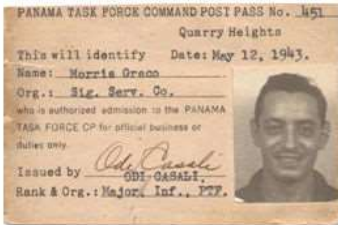
Vào một thời điểm ngẫu nhiên, bên cần xác nhận sẽ gửi một challenge mới để kiểm tra sự hợp lệ của kết nối.

Thông tin bí mật được chia sẻ giữa 2 bên có thể được lưu dưới dạng ký tự rõ nên rất dễ bị phát hiện và tấn công.

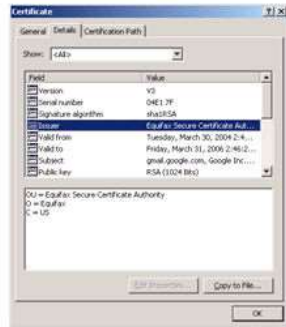
Chứng chỉ (Certificates)

Chứng chỉ điện tử là một dạng dữ liệu số chứa các thông tin để xác định một thực thể (thực thể có thể là một cá nhân, một server, một thiết bị hay phần mềm...)

Trong cuộc sống chúng ta sử dụng CMND hay hộ chiếu. Trong máy tính chúng ta sử dụng chứng chỉ số.



Giấy CMND



Chứng chỉ số được minh họa bởi Windows



Mô hình xử lý chứng thực bằng chứng chỉ

Mutual authentication

Mỗi thành phần trong một giao tiếp điện tử có thể xác nhận thành phần kia

Không chỉ xác nhận người dùng với hệ thống mà còn xác nhận tính hợp lệ của hệ thống đối với người dùng.

Biosmetrics

Các thiết bị sinh học có thể cung cấp một cơ chế xác nhận an toàn rất cao bằng cách sử dụng các đặc tính về vật lý và hành vi của mỗi cá nhân để chứng thực.

- Được sử dụng ở các khu vực cần sự an toàn cao
- Chi phí cao

Cách thức hoạt động của Biometric:

- Ghi nhận đặc điểm nhận dạng sinh học
- Các đặc điểm nhận dạng của đối tượng được quét và kiểm tra

- Các thông tin về sinh học được phân tích và lưu lại thành các mẫu
- Kiểm tra
- Đối tượng cần được kiểm tra sẽ được quét
- Máy tính sẽ phân tích dữ liệu quét vào và đối chiếu với dữ liệu mẫu
- Nếu dữ liệu đối chiếu phù hợp thì người dùng được xác định hợp lệ và có quyền truy xuất vào hệ thống.

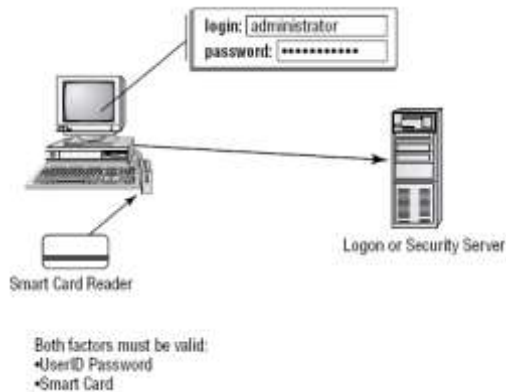
Một số dạng:

- Các đặc điểm vật lý (physical cha..)
- Dấu vân tay
- Hand geometry
- Quét khuôn mặt
- Quét võng mạc mắt
- Quét tròng đen mắt
- Các đặc tính về hành vi:
- Chữ ký tay
- Giọng nói

	
Dấu vân tay	Máy quét vồng mạc
	
Hand geometry	Máy quét chữ ký

Multi-factor

Khi một hệ thống sử dụng 2 hay nhiều phương pháp chứng thực khác nhau để kiểm tra việc user đăng nhập hợp lệ hay không thì được gọi là multi-factor. Một hệ thống vừa sử dụng smart card vừa sử dụng phương pháp chứng thực bằng username và password thì được gọi là một hệ thống chứng thực two-factor.



Chỉ danh của một cá nhân được xác định sử dụng ít nhất 2 trong các factors xác nhận sau:

- Bạn biết gì (một mật khẩu hay số PIN)
- Bạn có gì (smart card hay token)
- Bạn là ai (dấu vân tay, võng mạc...)
- Bạn làm gì (giọng nói hay chữ ký)

III. KIỂM TOÁN (Auditing)

Ghi nhận các sự kiện, các lỗi và quá trình xác nhận của người dùng..

Dùng để kiểm tra, theo dõi, lưu vết các hoạt động của người dùng đối với hệ thống

Auditing system

Thiết lập một hệ thống lưu vết nhằm lưu trữ các sự kiện cho phép chúng ta truy hồi lại các việc truy xuất, cả hợp lệ và không hợp lệ.

Logging: Tổ chức viện lưu trữ các thông tin: chứa ở đâu, dạng format nào, backup ra sao...

System scanning: Được dùng để kiểm tra và sửa chữa các điểm yếu của hệ thống. Quá trình này bao gồm việc sử dụng các công cụ để đánh giá những tiềm năng điểm yếu của hệ thống:

- Kiểm tra việc sử dụng mật khẩu
- Đánh giá khả năng truy cập mạng từ một hệ thống bên ngoài

- Theo dõi, nắm bắt các thông tin điểm yếu cả hệ điều hành và thiết bị phần cứng

Kiểm tra khả năng phản ứng của thiết bị bằng cách thiết lập các cuộc tấn công giả.

Chương 2

CÁC HÌNH THỨC TẤN CÔNG MẠNG PHỔ BIẾN

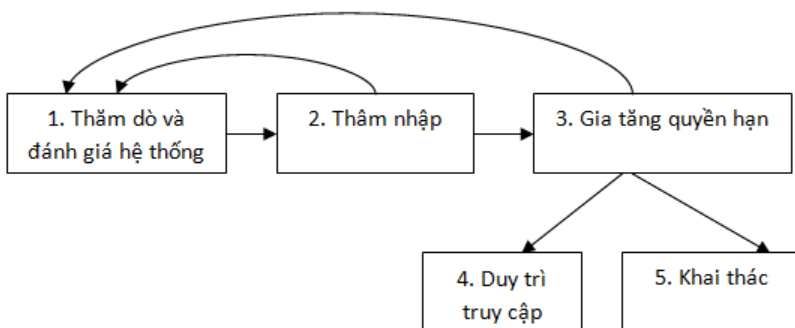
An ninh mạng luôn phát triển bởi vấn đề bảo mật dữ liệu lúc nào cũng là nhu cầu thiết yếu và các kỹ thuật tấn công ngày càng đa dạng và phong phú. Tuy có rất nhiều phương thức tấn công nhưng có thể tạm xếp chúng vào những nhóm như sau :

- Theo mục tiêu tấn công : Ứng dụng, Mạng hay cả hai
- Theo cách thức tấn công : chủ động (active) hay thụ động (passive)
- Theo phương pháp tấn công : có nhiều loại ví dụ như bẻ khóa, khai thác lỗi phần mềm hay hệ thống, mã nguy hiểm ...

Tuy nhiên ranh giới giữa các nhóm này dần khó nhận ra vì những cách tấn công ngày nay ngày càng phức tạp, tổng hợp.

I. Minh họa khái quát một kịch bản tấn công

Tùy thuộc vào mục tiêu tấn công mà Hacker sẽ có những kịch bản tấn công khác nhau. Ở đây chúng ta chỉ minh họa một dạng kịch bản tổng quát để tấn công vào hệ thống.



Hình II.1: Các bước cơ bản của một cuộc tấn công

- Bước 1: Tiến hành thăm dò và đánh giá hệ thống
- Bước 2: Thực hiện bước thăm nhập vào hệ thống. Sau đó có thể quay lại bước 1 để tiếp tục thăm dò, tìm thêm các điểm yếu của hệ thống.
- Bước 3: Tìm mọi cách để gia tăng quyền hạn. Sau đó có thể quay lại bước 1 để tiếp tục thăm dò, tìm thêm các điểm yếu của hệ thống hoặc sang bước 4 hay bước 5.
- Bước 4: Duy trì truy cập, theo dõi hoạt động của hệ thống
- Bước 5: Thực hiện các cuộc tấn công (ví dụ từ chối dịch vụ,...)

II. Tấn công chủ động

Là những dạng tấn công mà kẻ tấn công trực tiếp gây nguy hại tới hệ thống, mạng và ứng dụng (khống chế máy chủ, tắt các dịch vụ) chứ không chỉ nghe lén, hay thu thập thông tin.

Những dạng tấn công phổ biến như DoS, DDoS, Buffer overflow, IP spoofing ...

Dos

Tấn công từ chối dịch vụ, viết tắt là DoS (Denial of Service), là thuật ngữ gọi chung cho những cách tấn công khác nhau về cơ bản làm cho hệ thống nào đó bị quá tải không thể cung cấp dịch vụ, hoặc phải ngưng hoạt động. Kiểu tấn công này chỉ làm gián đoạn hoạt động chứ rất ít khả năng đánh cắp thông tin hay dữ liệu.

Thông thường mục tiêu của tấn công từ chối dịch vụ là máy chủ (FTP, Web, Mail) tuy nhiên cũng có thể là router, switch.

Tấn công từ chối dịch vụ không chỉ là tấn công qua mạng mà còn có thể là tấn công ở máy cục bộ, hay trong mạng cục bộ còn gọi là local DoS against hosts (dựa vào NetBIOS, fork() bomb).

Ban đầu tấn công từ chối dịch vụ xuất hiện khai thác sự yếu kém của giao thức TCP là DoS, sau đó phát triển thành tấn công từ chối dịch vụ phân tán DDoS (Distributed DoS) và mới xuất hiện là phương pháp tấn công từ chối dịch vụ phân tán phản xạ DRDoS (Distributed Reflection DoS).

Chúng ta cũng có thể phân nhỏ tấn công từ chối dịch vụ ra thành cách dạng Broadcast storm, SYN, Finger, Ping, Flooding ...

Hai vấn đề của tấn công từ chối dịch vụ là :

- Việc sử dụng tài nguyên (resource consumption attacks) của số lượng lớn yêu cầu làm hệ thống quá tải. Các tài nguyên là mục tiêu của tấn công từ chối dịch vụ bao gồm: Bandwidth (thường bị tấn công nhất), Hard disk (mục tiêu của bomb mail), RAM, CPU ...
- Có lỗi trong việc xử lý đối với các string, input, packet đặc biệt được attacker xây dựng (malformed packet attack). Thông thường dạng tấn công này sẽ được áp dụng với router hay switch. Khi nhận những packet hay string dạng này, do phần mềm hay hệ thống bị lỗi dẫn đến router hay switch bị crash...

Tấn công từ chối dịch vụ không đem lại cho attacker quyền kiểm soát hệ thống nhưng nó là một dạng tấn công vô cùng nguy hiểm đặc biệt là với những giao dịch điện tử hay thương mại điện tử. Những thiệt hại về tiền và danh dự, uy tín là khó có thể tính được. Nguy hiểm tiếp theo là rất khó để phòng dạng tấn công này. Thông thường chúng ta chỉ biết khi đã bị tấn công.

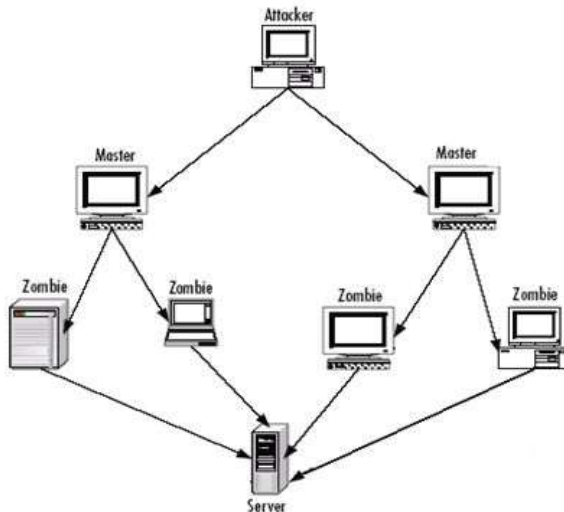
Đối với những hệ thống bảo mật tốt tấn công từ chối dịch vụ được coi là phương pháp cuối cùng được attacker áp dụng để triệt hạ hệ thống.

DDoS

Tấn công từ chối dịch vụ phân tán thực hiện với sự tham gia của nhiều máy tính. So với DoS mức độ nguy hiểm của DDoS cao hơn rất nhiều. Tấn công DDoS bao gồm hai thành phần :

- Thành phần thứ nhất là các máy tính gọi là zombie (thông thường trên Internet) đã bị hacker cài vào đó một phần mềm dùng để thực hiện tấn công dưới nhiều dạng như UDP flood, hay SYN flood ... Attacker có thể sử dụng kết hợp với spoofing để tăng mức độ nguy hiểm. Phần mềm tấn công thường dưới dạng các daemon.
- Thành phần thứ hai là các máy tính khác được cài chương trình client. Các máy tính này cũng như các zombie tuy nhiên attacker nắm quyền kiểm soát cao hơn. Chương trình client cho phép attacker gửi các chỉ thị đến daemon trên các zombie.

Khi tấn công attacker sẽ dùng chương trình client trên master gửi tín hiệu tấn công đồng loạt tới các zombie. Daemon process trên zombie sẽ thực hiện tấn công tới mục tiêu xác định. Có thể attacker không trực tiếp thực hiện hành động trên master mà từ một máy khác và sau khi phát động tấn công sẽ cắt kết nối với các master để đề phòng bị phát hiện.



Thông thường mục tiêu của DDoS là chiếm dụng bandwidth gây nghẽn mạng.

Các công cụ thực hiện có thể tìm thấy như Tri00 (WinTrinoo), Tribe Flood Network (TFN hay TFN2k), Shaft ...

Hiện nay còn phát triển các dòng virus, worm có khả năng thực hiện DDoS.

Buffer Overflows

Đây là một dạng tấn công làm tràn bộ đệm của máy victim. Buffer Overflows xuất hiện khi một ứng dụng nhận nhiều dữ liệu hơn chương trình chấp nhận. Trong trường hợp này, ứng dụng có thể bị ngắt. Khi chương trình bị ngắt có thể cho phép hệ thống gửi dữ liệu với quyền truy cập tạm thời đến những mức có đặc quyền cao hơn vào hệ thống bị tấn công. Nguyên nhân của việc bị tràn bộ đệm này là do lỗi chương trình.

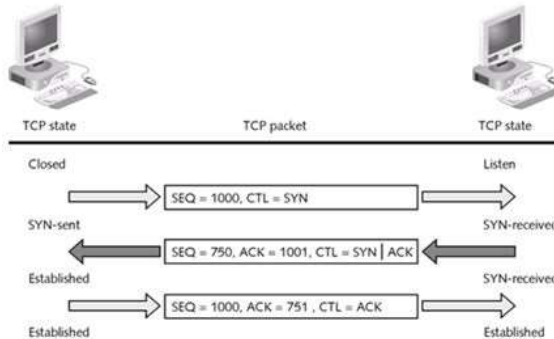
SYN Attacks

Là một trong những dạng tấn công kinh điển nhất. Lợi dụng điểm yếu của bắt tay ba bước TCP. Việc bắt tay ba bước như sau :

Bước 1 : client gửi packet chứa cờ SYN

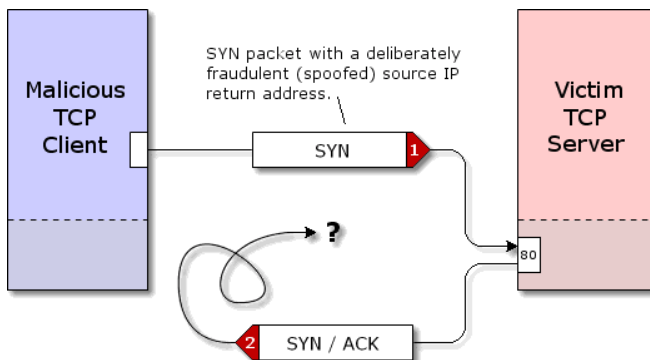
Bước 2 : server gửi trả client packet chức SYN/ACK thông báo sẵn sàng chấp nhận kết nối đồng thời chuẩn bị tài nguyên phục vụ kết nối, ghi nhận lại các thông tin về client.

Bước 3 : client gửi trả server ACK và hoàn thành thủ tục kết nối.

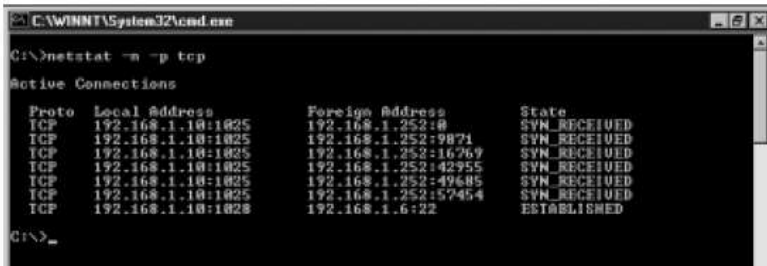


Khai thác lỗi của cơ chế bắt tay 3 bước của TCP/IP. Vấn đề ở đây là client không gửi trả cho server packet chứa ACK việc này gọi là half-open connection (client chỉ mở kết nối một nửa). Và với nhiều packet như thế server sẽ quá tải do tài nguyên có hạn. Khi đó có thể các yêu cầu hợp lệ sẽ không được đáp ứng. Việc này tương tự việc máy tính bị treo do mở quá nhiều chương trình cùng một lúc.

- Máy tính khởi tạo kết nối sẽ gửi một thông điệp Syn
- Máy nhận được sẽ trả lời lại SYN và một ACK
- Máy tính khởi tạo không trả lời thông điệp cuối dùng ACK của hoàn qui trình tạo kết nối
- Do vậy máy nhận được sẽ đợi một khoảng thời gian dài trước khi xóa kết nối
- Khi số lượng tạo kết nối SYN này quá nhiều sẽ làm cho hàng đợi tạo kết nối bị đầy và không thể phục vụ các yêu cầu kết nối khác



Để nhận biết tấn công SYN có thể dùng lệnh netstat -n -p tcp.



```
C:\WINNT\System32\cmd.exe
C:\>netstat -n -p tcp

Active Connections

Proto Local Address          Foreign Address         State
TCP   192.168.1.10:1025       192.168.1.252:10       SYN_RECEIVED
TCP   192.168.1.10:1025       192.168.1.252:9871     SYN_RECEIVED
TCP   192.168.1.10:1025       192.168.1.252:16769     SYN_RECEIVED
TCP   192.168.1.10:1025       192.168.1.252:42955     SYN_RECEIVED
TCP   192.168.1.10:1025       192.168.1.252:49685     SYN_RECEIVED
TCP   192.168.1.10:1025       192.168.1.252:57454     SYN_RECEIVED
TCP   192.168.1.10:1028       192.168.1.6:22         ESTABLISHED

C:\>
```

- Chúng ta sẽ chú ý trạng thái SYN_RECEIVED của các connection. Tuy nhiên tấn công SYN thường đi chung với IP spoofing. Cách attacker thường sử dụng là random source IP, khi đó server thường không nhận được ACK từ các máy có IP không thật, đồng thời server có khi còn phải gửi lại SYN/ACK vì nghĩ rằng client không nhận được SYN/ACK. Lý do tiếp theo là tránh bị phát hiện source IP, khi đó nhân viên quản trị sẽ block source IP này.

Giải pháp:

- Giảm thời gian chờ đợi khởi tạo kết nối. Việc này có thể sinh ra lỗi từ chối dịch vụ đối với máy từ xa có băng thông thấp truy xuất đến.
- Tăng số lượng các cố gắng kết nối
- Sử dụng tường lửa để gửi gói ACK cho máy nhận để chuyển kết nối đang thực hiện sang dạng kết nối thành công.

Spoofing

Truy cập vào hệ thống bằng cách giả danh (sử dụng chỉ danh đánh cắp của người khác, giả địa chỉ MAC, IP...)

Là phương pháp tấn công mà attacker cung cấp thông tin chứng thực hoặc giả dạng một user hợp lệ để truy cập bất hợp lệ vào hệ thống. Tuy nhiên trong vài trường hợp việc cấu hình hệ thống sai cũng có thể gây hậu quả tương tự. Ví dụ cấu hình hệ thống có lỗi cho user có quyền cao hơn quyền được phép mà user này không hề cố ý giả mạo.

Có nhiều loại tấn công bằng spoofing. Trong đó có "blind spoofing" attacker chỉ gửi thông tin giả mạo đi và đoán kết quả trả về. Ví dụ IP spoofing sau khi gửi packet giả mạo đi attacker không nhận được trả lời. Dạng thứ hai cần quan tâm là "informed spoofing" attacker kiểm soát truyền thông cả hai hướng.

Việc ăn cắp thông tin chứng thực (user, password) và sau đó sử dụng lại thực chất không phải là spoofing tuy nhiên có cùng kết quả tương tự.

Tấn công bằng cách giả mạo thường được nhắc đến nhất là IP spoofing và ARP spoofing hay còn gọi là ARP poisoning.

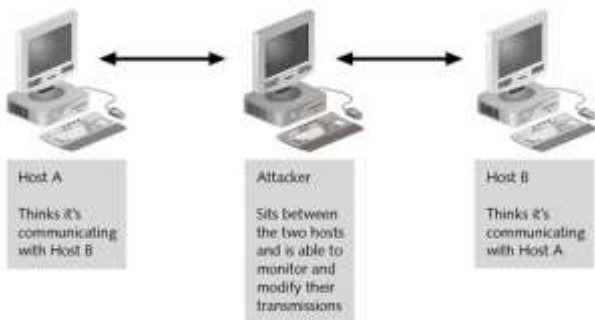
Việc giả mạo IP xảy ra do điểm yếu của giao thức TCP/IP. Giao thức TCP/IP không hề có tính năng chứng thực địa chỉ packet nhận được có phải là địa chỉ đúng hay là địa chỉ giả mạo. Một IP address được coi như là một máy tính (thiết bị) duy nhất kết nối vào mạng. Và do đó cách máy tính có thể giao tiếp với nhau mà không cần kiểm tra. Tuy nhiên chúng ta có thể khắc phục bằng cách sử dụng firewall, router, các giao thức và thuật toán chứng thực ... Việc thực hiện giả mạo IP có thể bằng cách sử dụng Raw IP.

ARP poisoning cách tấn công nhằm thay đổi ARP entries trong ARP table nhờ đó có thể thay đổi được nơi nhận thông điệp. Các tấn công này áp dụng với LAN switch.

Man in the Middle Attacks

Kẻ tấn công sẽ đứng giữa kênh truyền thông của 2 máy tính để xem trộm thông tin và thậm chí có thể thay đổi nội dung trao đổi giữa 2 máy tính.

Trong khi đó cả 2 máy tính đều nghĩ rằng mình đang kết nối trực tiếp với máy tính kia



Cách tấn công Man in the Middle

- Tấn công ARP
- ICMP Redirect

- **Chỉnh thông tin trong DNS**

Relay Attacks

Sử dụng công cụ để ghi nhận tất cả thông tin trao đổi khi một máy tính nào đó truy xuất đến Server.

Sau đó sử dụng các thông tin bắt được trên mạng để kết nối lại đến Server đó.

Là kỹ thuật mà attacker khi nắm được một số lượng packet sẽ sử dụng lại những packet này sau đó. Ví dụ attacker có được packet chứa password của một user. Password này đã được mã hóa và attacker không biết được. Tuy nhiên hệ thống chứng thực không có chức năng kiểm tra session time hay hệ thống có TCP Sequence number kém. Attacker sẽ thực hiện bypass authenticate bằng cách gửi packet một lần nữa hay còn gọi là replay.

Dumpster diving

Dumpster diving là thuật ngữ mô tả việc tấn công bằng cách thu lượm thông tin từ những thứ tưởng như không còn giá trị. Ví dụ attacker có thể có được nhiều thông tin từ "Recycle bin", từ giấy tờ chúng bỏ đi ...

Social Engineering

Sử dụng cách tấn công bằng cách lường gạt người khác thay vì sử dụng các công cụ máy tính.

Khai thác sự tin cậy hay nhẹ dạ của con người để tìm ra các thông tin quan trọng

Giải pháp: Đào tạo, hướng dẫn người dùng nên cảnh giác

III. Tấn công thụ động

Dò tìm lỗ hổng(Vulnerability Scanning)

Kỹ thuật dùng các công cụ quét để tìm ra điểm yếu tấn công

Sử dụng các công cụ quét cổng để thăm dò và phát hiện các thông tin của hệ thống như hệ điều hành, phiên bản, các ứng dụng triển khai...

Attacker sẽ kiểm tra để hy vọng tìm ra một cửa nào không khóa hoặc dễ dàng phá mà không bị phát hiện.

- **Nmap**

NMAP là viết tắt của Network MAPper. Ban đầu NMAP được thiết kế chủ yếu dành cho system admin nhằm scan những mạng có nhiều máy tính để biết máy nào đang hoạt động, các service nó đang chạy và hệ điều hành đang sử dụng.

NMAP hỗ trợ nhiều kỹ thuật scan bao gồm UDP, TCP, TCP SYN (half open), FTP proxy (bounce attack), ICMP (ping sweep), FIN, ACK sweep, Xmas tree, SYN sweep, IP protocol ... Có thể dùng xác định các thông tin của máy ở xa ví dụ như OS qua TCP/IP fingerprinting.

Công cụ NMAP có thể dễ dàng tìm trên Internet và được cài đặt mặc định trong các hệ điều hành Unix.

Một số chương trình có giao diện đồ họa nhưng ở đây chỉ chú ý vào việc sử dụng dạng command line.

Cú pháp chuẩn như sau :

nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>

Scan type bao gồm :

- -sS : TCP SYN
- -sT : TCP connect()
- -sU : UDP scans
- -sO :IP protocol
- -sF -sX -sN : stealth FIN, Xmas tree, Null scan
- -sP : ping scanning
- -sV : version detection

Các option chính như sau :

- -PA [portlist] sử dụng TCP ACK ping xem danh sách cách host đang hoạt động
- -PS [portlist] tương tự -PA nhưng dùng SYN (connection request)
- -PU [portlist] dùng UDP
- -p port/range of ports

Xác định mục tiêu : có thể là IP, danh sách IP, domain name, địa chỉ mạng ... hoặc nhập vào từ file với option -i

nmap 172.29.8.1, nmap 172.29.8.1 -255, nmap 172.29.8.1/24

nmap www.microsoft.com/24

Ping scanning và port scanning : mặc định NMAP dùng cách quét ICMP (ICM sweep) và TCP port 80 ACK sweep. Dùng loại scan là -sP cho ping scanning. Để bỏ ping sweep dùng -PO, dùng ICMP ping sweep dùng option -PI. Thông thường nếu dùng ICMP ping sweep sẽ bị chặn bởi firewall vì thế chúng ta sẽ phải dùng ACK sweep để kiểm tra host có hoạt động hay không với thông số -PT. Để xác định port cụ thể ví dụ -PT32453.

Với port scanning có thể dùng với ví dụ như sau :

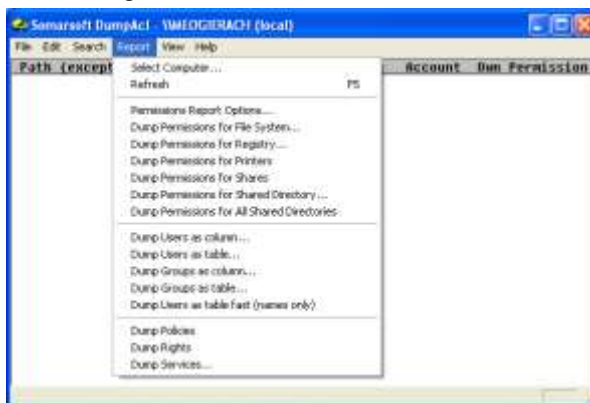
nmap -sS -p 22, 53, 80, 110, 143 192.168.*.1 -127 dùng scan port

OS scanning : dùng kiểm tra hệ điều hành.

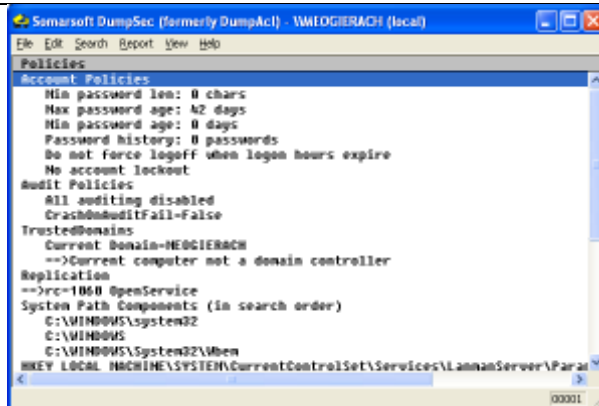
nmap -sS -O www.microsoft.com/24 dùng kiểm tra OS

- **DumpACL/DumpSec**

Là một chương trình Windows NT của Sotarsoft cho phép xem các quyền và thông tin cấu hình của file system, registry, printers nhờ đó có thể phát hiện các lỗ hổng bảo mật.



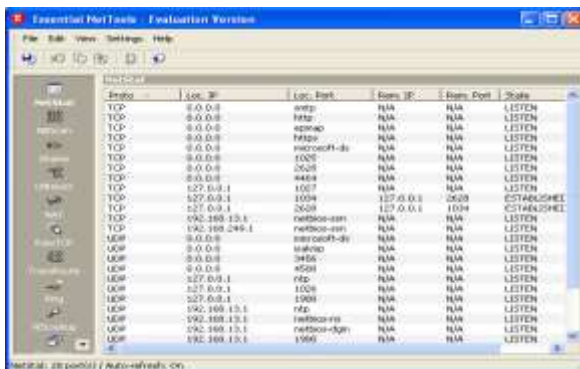
Ví dụ dump policies như sau :



• Essnetial NetTools

Là một bộ công cụ bao gồm netstat, nslookup, tracer, ping ...

Cách sử dụng tương đối dễ, hướng dẫn đầy đủ.



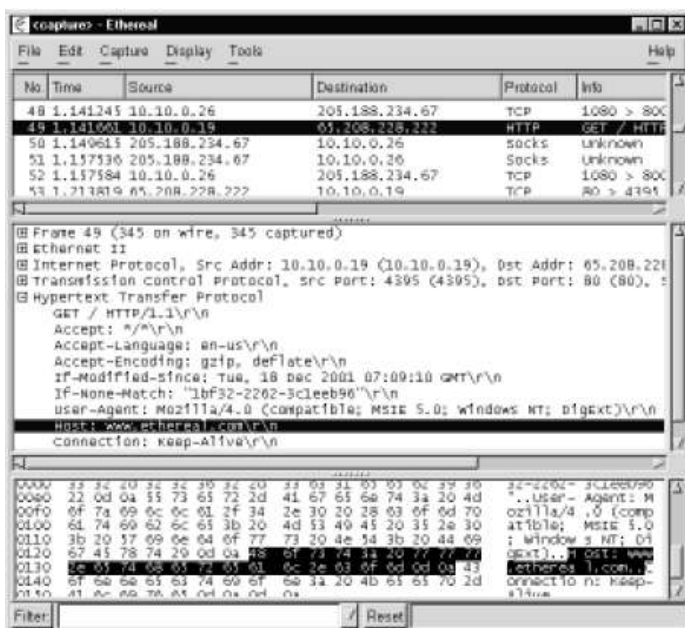
Sử dụng phần mềm để đón bắt các thông tin quan trọng (ví dụ tên truy cập, mật khẩu, cookie) truyền trên mạng mà không được mã hóa hoặc chỉ sử dụng những cơ chế mã hóa đơn giản.

Các quản trị mạng có thể sử dụng các công cụ sniff để xem xét và đánh giá lưu thông mạng (**)

Một số công cụ phổ biến :

- Giới thiệu công cụ Ethereal

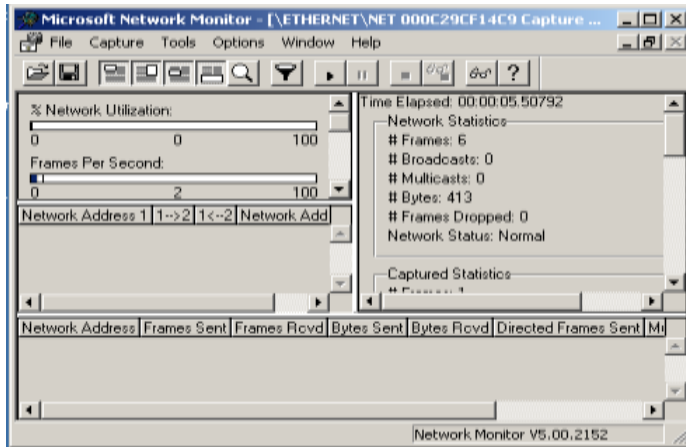
Là một trong những công cụ "phân tích giao thức" protocol analyzer mới nhất hiện nay, phát triển năm 1998. Ethereal có cả phiên bản cho Unix/Linux và Windows. Một khi thực hiện bắt gói tin, packet sẽ được giữ trong buffer và sau đó được hiển thị lên màn hình. Một tính năng của Ethereal là live decodes khá khác với các chương trình khác. Hầu hết các chương trình bắt gói tin không thể decode ngay packet cho đến khi dừng việc bắt gói tin. Chúng ta có thể thấy điều này qua Network monitor của Windows sẽ trình bày sau. Tuy nhiên đây cũng là tính năng không tốt lắm nếu lưu lượng mạng khá nhiều 10000 packet chẳng hạn mà không thực hiện biện pháp lọc gói nào. Khi đó chúng ta không thể nào theo dõi kịp các thông tin trình bày.



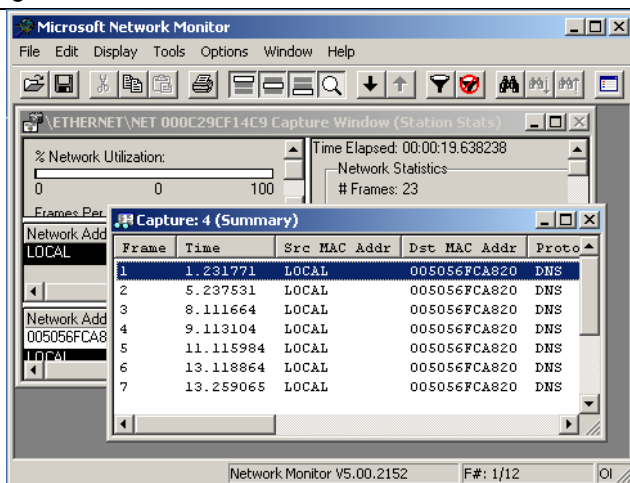
- **Giới thiệu công cụ Network monitor của Windows**

Cài đặt Start/Setting/Control panel/AddRemove program/AddRemove Windows components/Managenent and Monitoring tools.

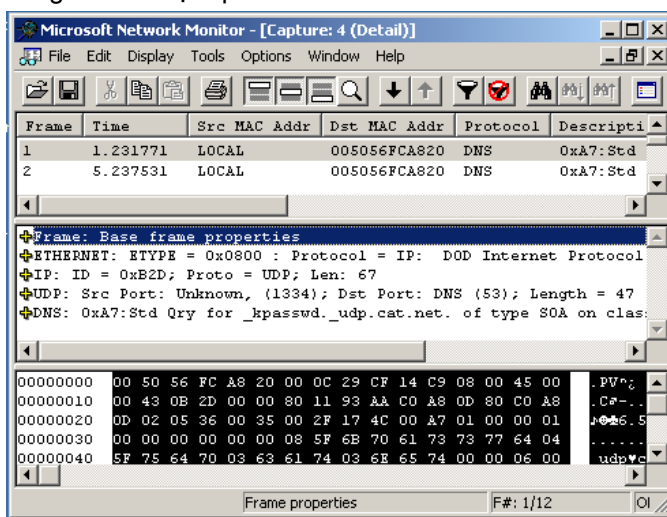
Chạy chương trình :



Sau khi chọn Network interface nhấn start capture để bắt gói tin. Nhấn biểu tượng Stop and View capture để xem các gói tin bắt được. Ngay sau khi bắt được chúng ta đang ở panel đầu là panel liệt kê tóm tắt.



Bỏ chọn Zoom panel (thanh toolbar hình kính lúp) để xem cả 3 panel của các gói tin đã bị capture như sau :



Panel thứ hai là thông tin chi tiết và panel cuối cùng biểu diễn dưới dạng hex. Dùng Edit/Display filter (thanh toolbar hình cái phễu) để lọc các gói tin.

- **Giới thiệu công cụ TCPDump**

Là công cụ phân tích mạng phổ biến trong môi trường Unix hay Linux. TCPDump hỗ trợ các giao thức TCP, UDP, IPv4 và ICMP. Ngoài ra còn hỗ trợ các dạng dữ liệu của các ứng dụng phổ biến. Hầu hết chương trình TCPDump phải chạy với quyền root hay được setuid là root.

Cú pháp TCPDump như sau :

Tcpdump [-adeflnNOpqRStuvX] [-c count] [-C file_size] [-F file] [-i interface] [-m module] [-r file] [-s snaplen] [-T type] [-U user] [-w file] [-E algo:secret] [expression]

Các lưu ý :

-c sẽ dừng khi bắt đủ số gói tin.

-C trước khi save raw packet vào file sẽ kiểm tra file hiện tại có kích thước lớn hơn file_size hay không. Nếu có thì mở một file mới với tên chỉ định là -w cộng với kích thước phía sau. Đơn vị của file_size là 1000000 bytes.

Xem thêm hướng dẫn sử dụng.

Password Attacks

Là phương pháp tấn công nhằm đoán ra password còn gọi là password guessing. Chúng ta có thể nghĩ ngay đến việc đoán password từ những thông tin liên quan đến user sử dụng nó : ngày sinh, tên

Có hai cách tấn công chính là brute-force attack và dictionary-based attack.

- **Brute Force Attacks**

- Sử dụng các công cụ đoán mật khẩu bằng các vét cạn
- Khả năng để tìm ra mật khẩu sẽ rất cao nếu mật khẩu đơn giản

- **Dictionary-Based Attacks**

- Các mật khẩu có trong các từ trong tự điển rất dễ bị phá mật khẩu
- Cách phá mật khẩu sử dụng một danh sách các từ nằm trong tự điển đã được tính giá trị băm trước.
- Danh sách các từ và giá trị băm có thể tìm thấy trên Internet

Malicious code attack

- **Virus**

Virus, Worm và Trojan horse được gọi chung là những đoạn mã nguy hiểm. Nó có thể chiếm dụng tài nguyên làm chậm hệ thống, hoặc làm hư hệ thống.

Virus là những chương trình được thiết kế để phá hoại hệ thống ở cả mức hệ điều hành và ứng dụng

- **Trojan Horses**

Trojan horse là một loại chương trình có vẻ an toàn và hữu ích nhưng thực sự bên trong của nó lại được nhúng những đoạn mã nguy hiểm.

- **Logic Bombs**

Những đoạn mã được tích hợp vào các ứng dụng và có thể được thực hiện để tấn công khi thỏa mãn một số điều kiện nào đó (ví dụ các Script hay ActiveX được tích hợp trong các trang Web).

Là một loại malware thường được attacker để lại trong hệ thống có tính năng tương tự "bom hẹn giờ". Logic bomb khi gặp những điều kiện nhất định sẽ phát huy tính năng phá hoại của nó. Một trong những logic bomb nổi tiếng là Chernobyl phát huy tính năng phá hoại của nó vào ngày 26/4. Một cách dùng của logic bomb mà attacker hay dùng là để hủy các chứng cứ của đợt tấn công khi admin hệ thống bắt đầu phát hiện đợt nhập

- **Worms**

Worm cũng là một dạng virus nhưng nó có khả năng tạo ra các bản sao để phát tán, lây lan qua mạng.

Một chương trình độc lập có thể tự nhân bản, lây lan qua mạng bằng nhiều cách nhưng thông thường nhất vẫn là e-mail và chat. Worm cũng có thể thực hiện các phá hoại nguy hiểm

- **Back door**

Một chương trình, một đoạn mã hay những cấu hình đặc biệt trên hệ thống mà chúng ta không biết cho phép attacker có thể truy cập mà không cần chứng thực hay login.

Chương 3

KỸ THUẬT KHAI THÁC WEBSITE

I. BẢO MẬT WEB

Bảo mật trên WEB Server

I.1.1 Điều khiển truy cập (Access Control)

Khi người dùng bất kỳ (anonymous) truy cập vào Web Server, Web Server sẽ sử dụng một tài khoản IUSER_<computename> để truy xuất tài nguyên.

Các người dùng truy cập vào Web Server với tài khoản riêng thì có quyền hạn tương ứng với quyền hạn của tài khoản được cấp trên Web Server.

Vì thế việc quản lý điều khiển truy cập rất quan trọng và cần được đặc biệt quan tâm. Thông thường ta chỉ nên cấp những quyền hạn thấp nhất có thể có để truy xuất đến tài nguyên trên Web Server.

I.1.2 Quản lý an toàn dữ liệu Web

Cấu trúc thư mục và dữ liệu web rất quan trọng trong việc bảo vệ một Web Server.

Thông thường ta có thể sử dụng một thư mục ảo hay ảnh xạ chứa dữ liệu Web trên một máy khác. Việc sử dụng thư mục ảo hay ảnh xạ ổ đĩa trên một máy khác có thể tạo điều kiện cho người thâm nhập tấn công vào các phần khác của hệ thống khi họ tấn công được Web Server.

Trong trường hợp người dùng phải truy cập các tài nguyên trên một hệ thống khác từ Web, chẳng hạn một cơ sở dữ liệu, thì tốt nhất là nên có một bản sao một máy chủ CSDL và được đặt trong vùng DMZ.

1.1.3 Loại bỏ các đoạn mã có thể gây nguy hiểm

Cần bảo đảm rằng các kịch bản và các ứng dụng Web được triển khai trên web server không là các Trojans, các chương trình cửa sau, hoặc các đoạn mã không đáng tin cậy.

1.1.4 Lưu vết truy cập Web (Logging)

Việc lưu trữ, theo dõi và giám sát các hoạt động của Web Server vô cùng quan trọng để phát hiện kịp thời các tấn công vào Web Server.

Lưu lại các dữ liệu:

- Thi hành các kịch bản
- Ghi thông tin vào các tập tin
- Truy cập dữ liệu không nằm trong thư mục, dữ liệu được cung cấp bởi Web

Tuy nhiên vấn đề khó khăn ở đây là việc theo dõi và giám sát hoạt động này rất mất thời gian. Vì thế ta có thể sử dụng hệ thống phát hiện thâm nhập tự động IDS để phát hiện và thông báo kịp thời khi có sự cố xảy ra.

1.1.5 Backup dữ liệu Web và bảo đảm tính nhất quán của thông tin

Mục tiêu của dịch vụ Web là cung cấp thông tin, vì vậy dữ liệu Web cần được bảo vệ tránh việc bị phá hỏng, sao chép, hay thay đổi nội dung.

Dữ liệu Web cần được backup thường xuyên (cả online và offline) để bảo đảm khả năng phục hồi nhanh chóng khi có sự cố xảy ra với máy chủ Web.

Ngoài ra cần bảo đảm sự toàn vẹn và không bị thay đổi bất hợp pháp của thông tin Web.

Kiểm tra các hành vi ghi dữ liệu lên Web server.

Định kỳ kiểm tra và ghi nhận khi có sự thay đổi thông tin.

Quản lý, phân quyền các truy xuất (từ mạng cục bộ, từ internet, dạng ứng dụng, người dùng...)

Thường xuyên cập nhật các bản vá lỗi.

1.1.6 Phát hiện và tắt các dịch vụ Web không mong muốn

Đôi khi một máy tính có cài đặt tính năng phục vụ web mà người dùng không biết (có thể do cơ chế cài đặt mặc định của hệ điều hành). Đây sẽ là lỗ hổng rất lớn cho phép kẻ tấn công thâm nhập vào, khai thác và sử dụng để tấn công vào các hệ thống khác.

Có nhiều cách để phát hiện:

- Tại bất kỳ một máy này, vào trình duyệt và bấm: <http://localhost>, hay <http://127.0.0.1>. Sau đó xem thông tin xuất hiện trên trình duyệt.
- Trên Windows ta cũng có thể tìm xem có tiến trình `inetinfo.exe` trong công cụ Task Manager hay không? Nếu có là Web server đang tồn tại và hoạt động.
- Tìm trong phần Service
- Thi hành `netstat -na` và kiểm tra xem có chương trình nào lắng nghe trên cổng 80.

Bảo mật trên WEB Client

Client truy cập các trang web bằng các công cụ Browser. Một số Browser phổ biến: Internet explorer, Netscape, Opera, Mozilla, ...

Phần mềm browser có thể truy xuất thông tin của người dùng và máy tính người dùng sử dụng để gửi cho Web server. Việc gửi thông tin này có thể do người dùng tự thực hiện hoặc bằng các đoạn mã từ Web Server (client không hề hay biết).

Các browser thường lưu các cookies (thông tin dạng text được mã hóa chứa các thông tin người dùng truy cập đến Server, Client sử dụng cookie để truy xuất) do Server gửi

Ngoài ra các trang web giả mạo các web site có uy tín mà người dùng thường sử dụng để an cắp cá thông tin các nhân mà người dùng khai báo khi truy cập. Ví dụ trang web <http://www.bank.vn> là trang web chính, và <http://www.banks.vn> là trang web mà hacker tạo ra để lừa người dùng (khi người dùng không nhớ rõ tên trang web hay không chú ý vì tên của 2 trang web có khác biệt rất nhỏ).

Cách giả mạo khác sử dụng ký tự @, bằng cách gửi các email với kết nối:

[@%77%77%77.%61%7A.%72%75/%70%70%64](http://www.bank.com)

liên kết này trong có về kết nối đến www.bank.com nhưng thực ra là nối nối đến địa chỉ IP: ... Vì thế quản trị mạng nên thông

báo với người dùng nên cẩn thận khi nhận được các email chứa liên kết Web mà URL có chứa ký tự @.

Một các khác là dùng các chương trình Trojan theo dõi khi người sử dụng web truy cập vào những địa chỉ ngân hàng, thương mại trực tuyến hợp lệ rồi bí mật ghi lại quá trình giao dịch để ăn cắp thông tin

Giao thức SSL và HTTPS

SSL được thiết kế bởi công ty Netscape và hiện nay trở thành chuẩn truyền thông an toàn của IETF.

Mục tiêu của SSL dùng để thiết lập một kênh truyền thông dữ liệu an toàn, bí mật và đáng tin cậy giữa Client và Server.

SSL rất thành công trong việc bảo vệ thông tin trang Web. Nghi thức SSL được sử dụng để bảo vệ các trang web truyền qua mạng còn được gọi là nghi thức HTTPS (hoạt động trên cổng TCP 443)

SSL cho phép các nhà phát triển ứng dụng cơ chế bảo mật cho các dịch vụ khác như mail, Telnet, FTP...



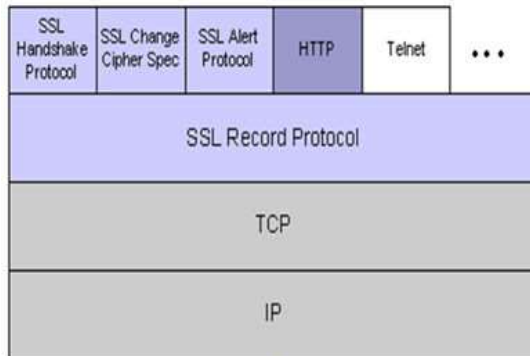
1.1.7 Nghi thức SSL

Nghi thức SSL hoạt động trên hạ tầng khóa công khai PKI. Vì thế SSL đòi hỏi máy chủ có sử dụng dịch vụ SSL cần cài đặt chứng chỉ xác nhận để client có thể xác nhận sự hợp lệ của Server.

Nghi thức SSL là một nghi thức cấp ứng dụng và nằm ở tầng trên cùng của mô hình lớp TCP/IP.

SSL độc lập với nghi thức ứng dụng mà nó bảo vệ, vì thế bất kỳ nghi thức cấp cao hơn SSL có thể được đặt trên nghi thức SSL. Vì thế các ứng dụng, nghi thức khác nhau có thể sử dụng các tính năng hỗ trợ bảo mật của SSL.

SSL gồm 2 phần: nghi thức bắt tay SSL và nghi thức SSL Record



Các thành phần của SSL

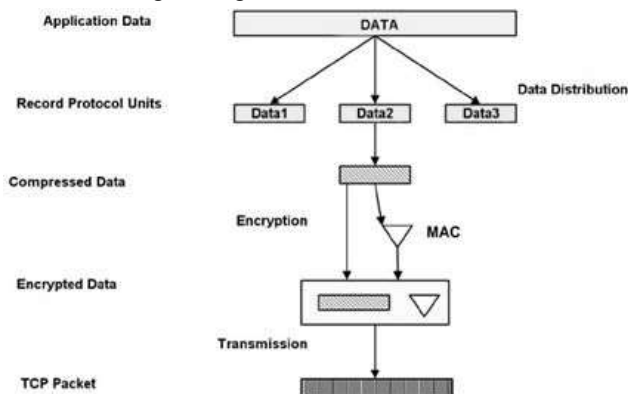
I.1.8 SSL Record

Phân mảnh thông điệp tại nơi gửi và sắp xếp lại tại nơi nhận

Kiểm tra và kiểm chứng sự toàn vẹn của thông điệp

Cho phép (chọn lựa) nén hay không nén thông điệp ở nơi gửi và giải nén thông điệp ở nơi nhận

Mã hóa bên gửi và giải mã bên nhận



Hoạt động của SSL Record

Hình trên mô tả hoạt động của SSL:

- Dữ liệu từ tầng ứng dụng đưa xuống sẽ được chia nhỏ thành những khối dữ liệu nhỏ.
- Sau đó khối dữ liệu nhỏ sẽ được nén lại để giảm kích thước.

- Tiếp theo khối dữ liệu nén sẽ được mã hóa. Đồng thời khối dữ liệu nén sẽ được băm để tạo ra một giá trị MAC dành để xác định tính toàn vẹn của thông tin.
- Sau đó khối liệu được mã hóa và MAC được gửi xuống tầng dưới để đóng gói thành các gói TCP.
- Khi đó bên nhận sẽ làm thao tác ngược lại để xác định tính toàn vẹn của thông tin và nhận được nội dung thông tin.

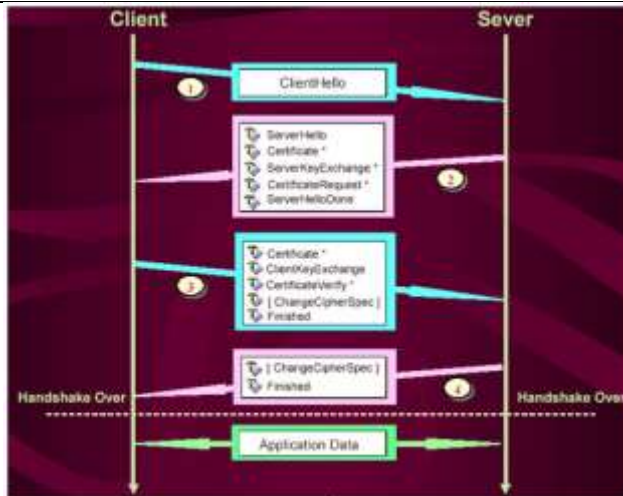
1.1.9 Nghi thức bắt tay SSL

Mục tiêu của nghi thức bắt tay:

- Xác nhận sự hợp lệ của các thành phần tham gia vào kênh an toàn SSL.
- Đàm phán thuật toán mã hóa và nghi thức xác nhận tính toàn vẹn của thông tin ,
- Khởi tạo và đồng ý khóa trung gian để mã hóa kênh an toàn
Có 2 nghi thức bắt tay xác nhận chính:
- Xác nhận một chiều: Client xác nhận sự hợp lệ của Server
- Xác nhận lẫn nhau: cả client và Sever cần xác nhận lẫn nhau

Tùy theo nhu cầu của ứng dụng mà chúng ta sẽ có cách chọn lựa nghi thức xác nhận phù hợp.

Hình dưới đây sẽ mô tả qui trình của nghi thức bắt tay xác nhận lẫn nhau:



Nghị thức bắt tay SSL

- Client gửi yêu cầu kết nối đến Server
- Server nhận yêu cầu và gửi thông điệp trả lời cho Client. Bên cạnh đó Server sẽ gửi chứng chỉ của mình cho Client, đồng thời yêu cầu client cung cấp chứng chỉ của Client.
- Khi nhận được thông tin phản hồi từ Server, client sẽ kiểm tra xem chứng chỉ của Server có hợp lệ hay không. Nếu hợp lệ client sẽ:
 - Trích khóa công khai của Server lấy trong chứng chỉ Server gửi đến
 - Gửi chứng chỉ của mình cho Server.
 - Tiếp theo Client sẽ gửi kèm các thông tin cần thiết về khóa trung gian sử dụng mã hóa, thuật toán mã hóa, cách thức chứng nhận thông tin ... (các thông tin này sẽ được mã hóa bằng khóa công khai của Server)
- Server nhận được thông điệp Client gửi, Server sẽ kiểm tra chứng chỉ của client có hợp lệ hay không. Nếu hợp lệ Server sẽ :
 - Trích khóa công khai của Client trong chứng chỉ
 - Sử dụng khóa bí mật của mình để giải mã thông tin Client gửi để biết được khóa trung gian truyền thông và các thông tin khác về thuật toán mã hóa, cách thức chứng nhận thông tin ... mà Client yêu cầu

- Nếu Server đồng ý sẽ gửi trả về thông điệp trên và mã hóa bằng khóa công khai lấy từ trong chứng chỉ của Client.
- Sau đó tất cả các thông tin trao đổi giữa Client và Server được mã hóa và bảo đảm tính bảo mật và toàn vẹn thông tin.

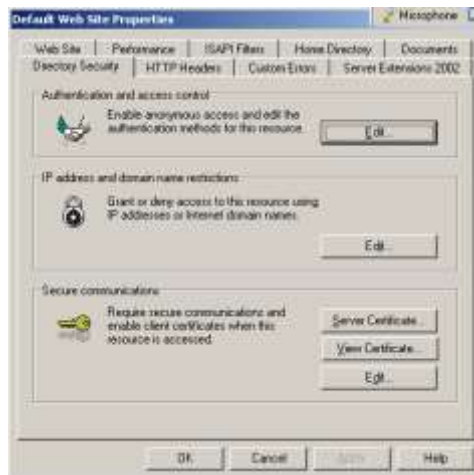
1.1.10 Cài đặt và cấu hình SSL trên IIS 6.0

Bước 1: Cài đặt và cấu hình CA Server trên một hệ thống máy tính, đăng ký Web Browser Certificate. (xem chương 4)

Bước 2: Thiết lập Certificate trên website.

Kích hoạt Web Server:

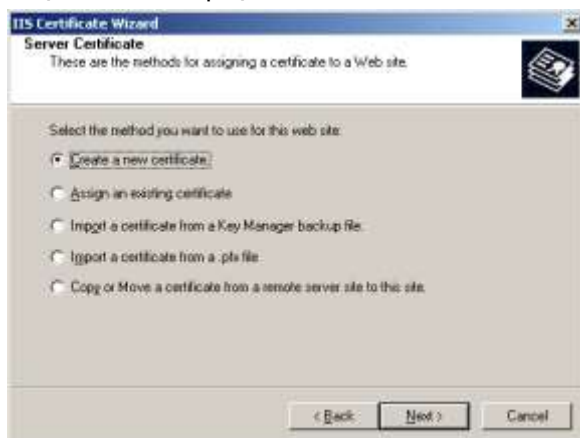
Start → Programs → Administrative Tools → Internet Information Services Manager. Nhấp phải chuột tại mục Default Web Site → chọn Properties.



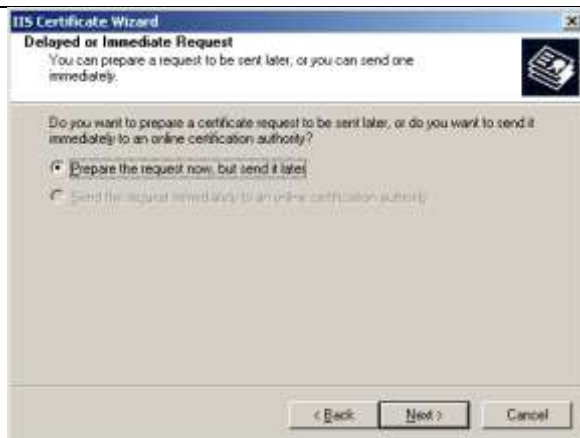
Tại hộp thoại Properties, chọn mục Tab Directory Security → Server Certificate.



Chọn Next để tiếp tục.



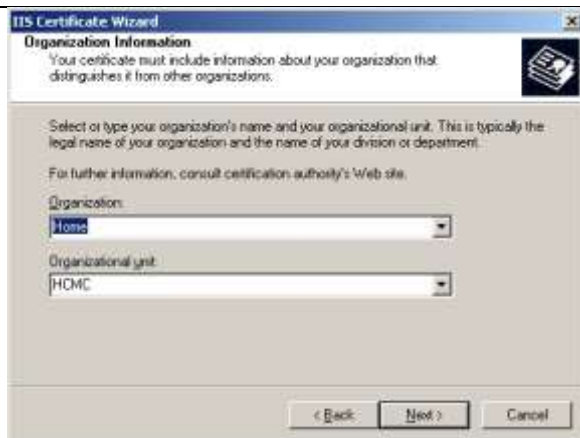
Tại cửa sổ Server Certificate, chọn mục Create a new certificate.



Tại cửa sổ Delayed or Immediate Request, chọn mục Prepare the request now, but send it later.



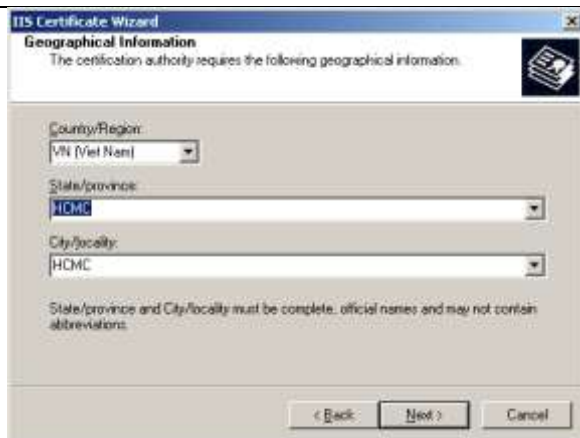
Tại cửa sổ Name and Security Settings, nhập vào tên cho chứng chỉ mới, chọn chiều dài bit dùng để mã hóa của chứng chỉ. Nhấp Next để tiếp tục.



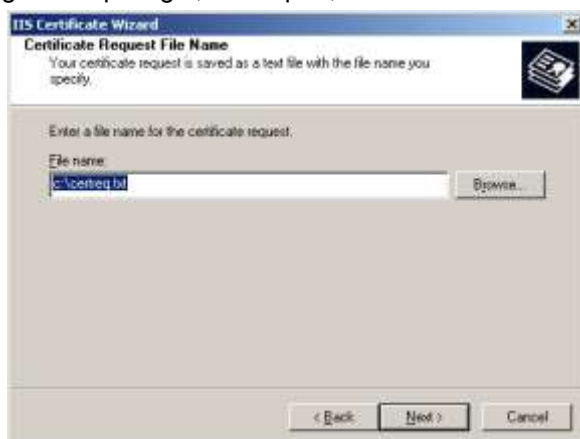
Tại cửa sổ Organization Information, nhập vào tên tổ chức và đơn vị của tổ chức, nhấn Next để tiếp tục.



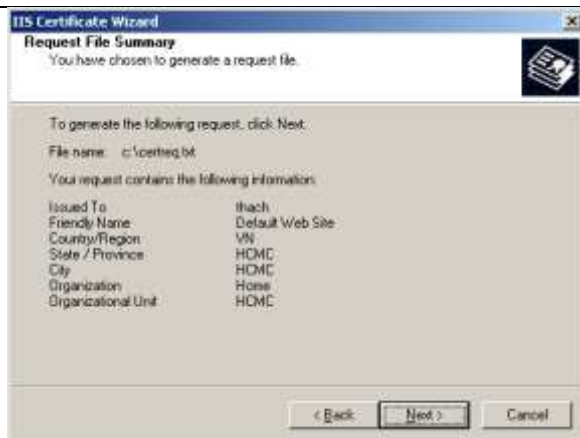
Tại cửa sổ Your Site's Common Name, nhập vào tên Website cần thiết lập SSL, nếu server có tồn tại trên Internet, chúng ta sẽ nhập vào một tên DNS hợp lệ.



Tại cửa sổ Geographical Information, nhập vào những thông tin về quốc gia, thành phố, ...



Tại cửa sổ Certificate Request File Name, nhập vào vị trí và tên tập tin được sử dụng để lưu trữ những thông tin về việc yêu cầu chứng chỉ. Tập tin này sẽ được chuyển lên cho CA Server và Import vào để thực hiện việc cấp chứng chỉ dạng offline. Nhấp Next để tiếp tục.



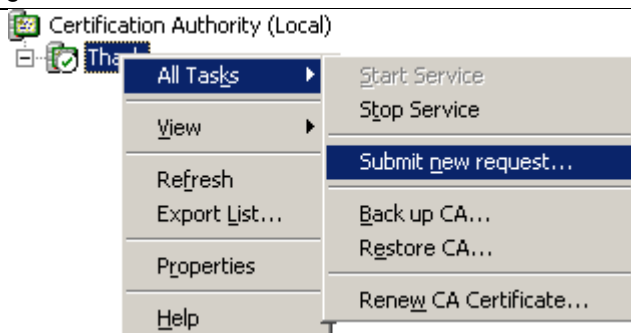
Cửa sổ Request File Summary tóm tắt lại những thao tác đã thực hiện. Chúng ta có thể quay trở lại để sửa đổi hoặc nhấp Next để thực hiện việc đăng ký.



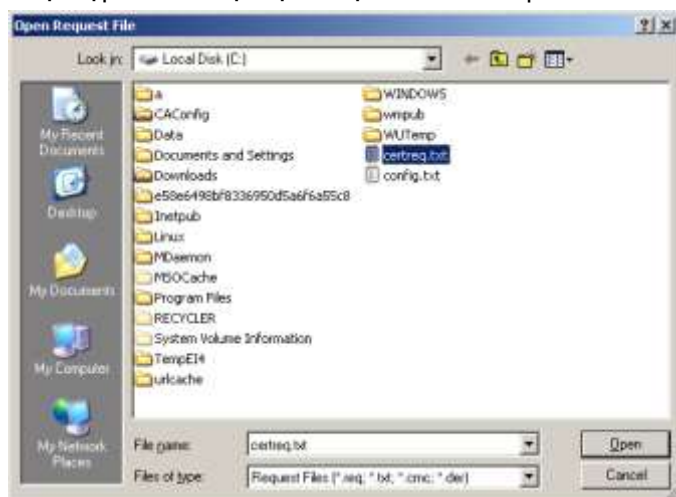
Chọn Finish để kết thúc quá trình đăng ký.

Bước 3: Import Website Certificate vào CA Server

Start → Programs → Administrative Tools → Certificate Authority. Nhấp phải chuột trên Certificate Server → All Tasks → Submit new request.



Chọn tập tin đã được tạo ra tại bước 2 → Open.



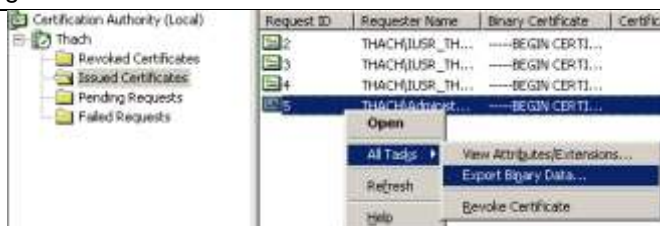
Khi chứng chỉ được Import vào, chứng chỉ sẽ được lưu tại mục Pending. Để kích hoạt chứng chỉ, chúng ta nhấp phải chuột trên chứng chỉ → All Task → Issue.



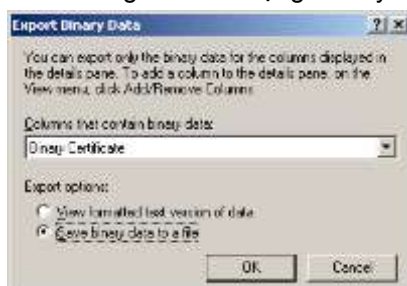
Bước 4: Export chứng chỉ đã cấp phát từ CA Server và cài đặt chứng chỉ tại Website cần thiết lập SSL.

Export chứng chỉ:

Chọn CA Server → Issued Certificates. Nhấp phải chuột tại chứng chỉ đã được cấp → All Tasks → Export Binary Data.



Lưu chứng chỉ theo dạng Binary.



Chọn đường dẫn lưu tập tin được Export → chọn Save.

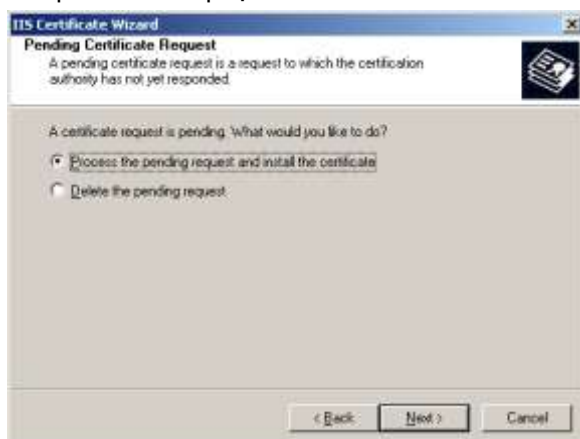


Khi chứng chỉ đã được Export, để Import chứng chỉ vào Website cần thiết lập SSL, chúng ta thực hiện các bước sau:

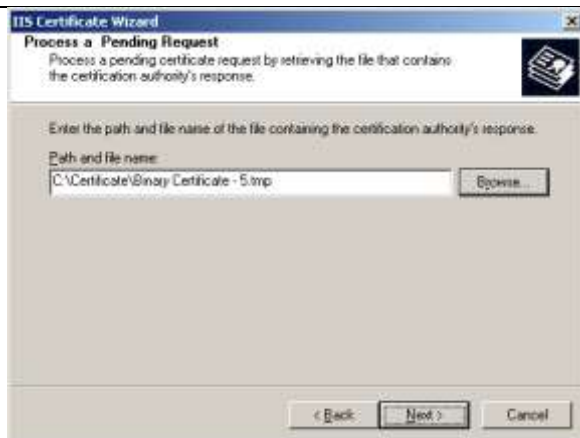
Start → Programs → Administrative Tools → Internet Information Services. Nhấp phải chuột tại Website cần thiết lập SSL → Properties → Chọn tab Directory Security → Server Certificate.



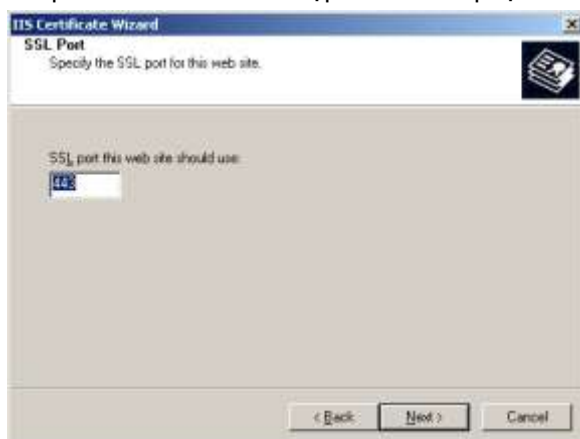
Nhấp Next để tiếp tục.



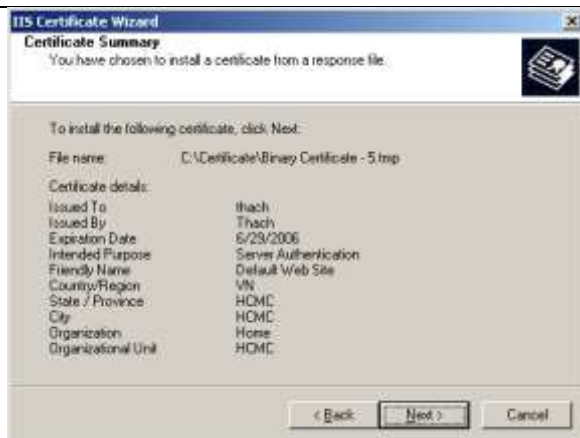
Tại cửa sổ Pending Certificate Request, chọn mục Process the pending request and install the certificate.



Tại cửa sổ Process a Pending Request, chọn tập tin đã được Export từ CA Server. Nhập Next để tiếp tục.



Chọn cổng dịch vụ SSL, mặc định là 443. Nhấp Next để tiếp tục.



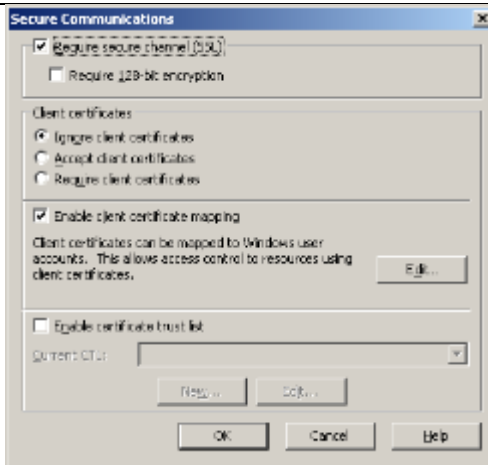
Cửa sổ Certificate Summary tóm tắt lại những thao tác đã thực hiện. Nhấp Next để tiếp tục hoàn tất quá trình cài đặt chứng chỉ.



Chọn Finish để kết thúc quá trình đăng ký chứng chỉ.

Bước 5: Thiết lập SSL và kiểm tra.

Start → Programs → Administrative Tools → Internet Information Services. Nhấp phải chuột trên Website cần thiết lập SSL → Properties → Chọn Tab Directory Security → Edit.



Tại hộp thoại Secure Communication, chọn mục →Require secure channel (SSL).

Kiểm tra:

Truy cập website theo địa chỉ qui định (<https://172.29.14.153>). Hộp thoại Security Alert sẽ cảnh báo mọi thông tin khi trao đổi giữa Web Client và Web Server sẽ không bị nhìn thấy. Chọn OK để tiếp tục.



Hộp thoại Security Alert tiếp tục cảnh báo về chứng chỉ đã được đăng ký còn hợp lệ và còn thời gian sử dụng. Nhấp Yes để tiếp tục.



Trang web được hiển thị trên Browser thông qua việc truyền thông SSL.



Các lỗ hổng bảo mật liên quan đến WEB và cách phòng chống

1.1.11 JavaScript

Ngôn ngữ được phát triển bởi Netscape để cho phép thi hành các đoạn mã thi hành được nhúng trong trang web.

Các chương trình có thể thi hành các chức năng ngoài khả năng kiểm soát của người dùng

- Theo dõi duyệt trang web
- Đọc mật khẩu và các tập tin hệ thống
- Đọc các tham số của browser

1.1.12 ActiveX

Công nghệ được Microsoft phát triển để thay thế công nghệ OLE (Object Linking and Embedding) và COM (Component Object Model).

Cung cấp khả năng liên kết các ứng dụng trên máy tính với nội dung của trang web

Cho phép thi hành các đoạn mã Visual Basic được tích hợp trong trang web thi hành trên máy cục bộ

ActiveX không thi hành trong một không gian giới hạn (Sandbox) như Java applet, vì vậy ActiveX đưa ra nhiều nguy cơ cho ứng dụng.

Giảm bớt nguy cơ ảnh hưởng của ActiveX

1.1.13 CGI

Mô tả các luật cho phép Web Server giao tiếp với các phần mềm khác trên máy chủ và ngược lại

Thường được dùng để cho phép Web Server truy xuất và trình bày thông tin trong CSDL lên trang web hay cho phép người dùng nhập thông tin từ trang web và lưu vào CSDL.

1.1.14 Cookies

Được thiết kế để mở rộng khả năng truy cập web của Browser- cung cấp trạng thái cho web

Thông điệp mà Web Servers cung cấp cho Web Browsers:

- Browser lưu trữ thông điệp trong một tập tin dạng Text
- Thông điệp này được gửi lại cho Server mỗi lần browser yêu cầu 1 trang từ server

Web server xác định một phiên làm việc của người dùng

Các điểm yếu của cookie:

- Cookies có thể dễ dàng bị lợi dụng để cung cấp các thông tin về người dùng mà không có sự đồng ý.
- Attacker convinces user to follow malicious hyperlink to targeted server to obtain the cookie through error handling process on the server
- User must be logged on during time of attack
- Cookies có thể được dùng để tìm hiểu các thói quen duyệt web, lấy đi thông tin tài khoản...

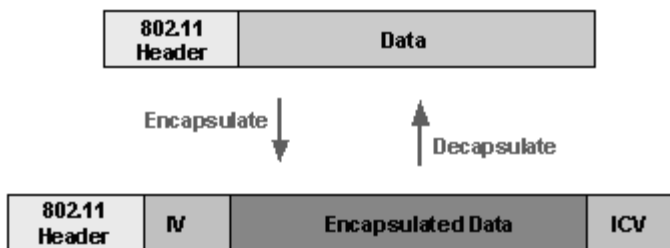
Chương 4

CÁC KỸ THUẬT KHAI THÁC LỖ HỎNG MẠNG KHÔNG DÂY

I. BẢO MẬT TRÊN HỆ THỐNG MẠNG KHÔNG DÂY

Giới thiệu

Mạng không dây dựa trên môi trường sóng để truyền dữ liệu nên các tin tặc rất dễ nghe lén và tấn công, do đó vấn đề bảo mật trong mạng không dây là quan trọng. Đầu tiên mạng không dây nội bộ theo chuẩn IEEE 802.11 bảo mật dùng thông số cấu hình SSID (Service Set ID). SSID có thể hiểu là tên của mạng không dây, kỹ thuật này hoạt động theo hai chế độ. Chế độ không bảo mật thì theo chu kỳ thời gian Access Point gửi broadcast SSID của mình đến các máy trạm không dây, máy trạm nhận các tín hiệu này từ đó quyết định chọn Access Point để kết nối thông qua SSID. Chế độ thứ hai là chế độ bảo mật thì Access Point không gửi thông tin SSID của mình, mà máy trạm muốn kết nối vào mạng phải có cùng giá trị SSID với Access Point.



Hình 3.23: Quá trình trao đổi SSID

Các chuẩn bảo mật trên hệ thống mạng không dây

I.1.1 WEP

Chuẩn IEEE 802.11b định nghĩa một protocol bảo mật WEP (Wired Equivalent Privacy) cho mạng không dây nội bộ. WEP được thiết kế cùng tăng bảo mật với mạng có dây, protocol này bảo mật bằng cách mã hóa

dữ liệu khi truyền từ điểm này đến điểm khác. WEP làm việc tại hai tầng thấp nhất trong mô hình tham chiếu OSI, sự đóng gói của WEP bao gồm những nội dung chính sau:

- Thuật toán mã hóa: RC4.
- Khóa mã hóa trên mỗi packet: 24bit IV (Initialization Vector) nối vào khóa chia sẻ.
- WEP cho phép IV (Initialization Vector) được dùng lại trên bất kỳ Frame nào.
- Tính nguyên vẹn dữ liệu được cung cấp bởi CRC-32.

I.1.2 WPA

Khi triển khai một hệ thống mạng Wireless, người ta đã đưa ra nhiều giải pháp giúp bảo mật trên hệ thống mạng. Với kỹ thuật bảo mật sử dụng WEP với nhiều tính năng không đảm bảo an toàn (dễ dàng bị mất key...), do đó Wifi Alliance đã đưa ra một phương thức khác nhằm tăng tính năng bảo mật trên mạng không dây, đó là WPA (Wifi Protected Access). WPA đưa ra một phương thức mã hóa mạnh mẽ hơn gọi là TKIP (Temporal Key Integrity Protocol). WPA cũng cho phép tùy chọn sử dụng AES (Advanced Encryption Standard) để mã hóa. WPA có hai chế độ khác nhau:

- WPA-Enterprise: Sử dụng cơ chế chứng thực 802.1X được thiết kế cho hệ thống mạng Infrastructure vừa và lớn.
- WPA-Personal: Sử dụng Preshared Key (PSK) để chứng thực và sử dụng cho hệ thống mạng Infrastructure nhỏ (SOHO – Small Office/Home Office)

Chương 5

CÁC KỸ THUẬT SỬ DỤNG TROJAN, WORM

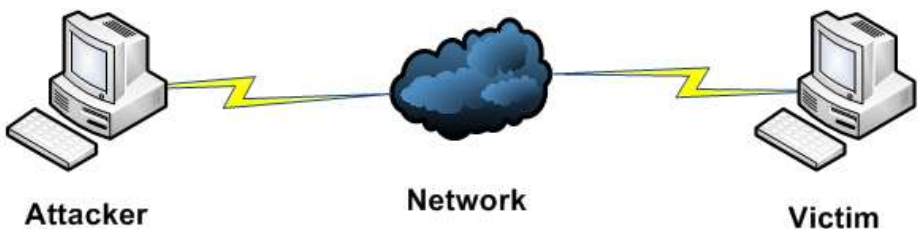
I. Kỹ thuật sử dụng Trojan:

I.1 Khái niệm Trojan:

Trojan Horse: đây là loại chương trình cũng có tác hại tương tự như virus chỉ khác là nó không tự nhân bản ra. Như thế, cách lan truyền duy nhất là thông qua các thư dây chuyền. Để trừ loại này người chủ máy chỉ việc tìm ra tập tin Trojan horse rồi xóa nó đi là xong. Tuy nhiên, không có nghĩa là không thể có hai con Trojan horse trên cùng một hệ thống. Chính những kẻ tạo ra các phần mềm này sẽ sử dụng kỹ năng lập trình của mình để sao lưu thật nhiều con trước khi phát tán lên mạng. Đây cũng là loại virus cực kỳ nguy hiểm. Nó có thể hủy ổ cứng, hủy dữ liệu.

I.2 Mô hình triển khai

Mô hình sau:



Tạo Trojan

Điều khiển Trojan:

- Truy xuất file hay thư mục trên máy Victim
- Tắt Firewall

- Quản lý các ứng dụng, dịch vụ,... trên máy Victim
- Xem màn hình máy Victim

Hướng dẫn thực hiện:

Tạo Trojan:

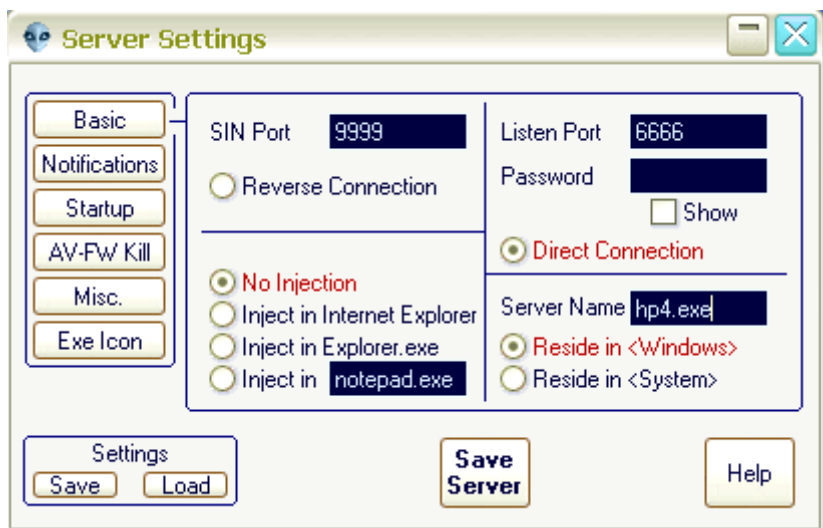
- Thực thi Beast Trojan



- Chọn Build Server



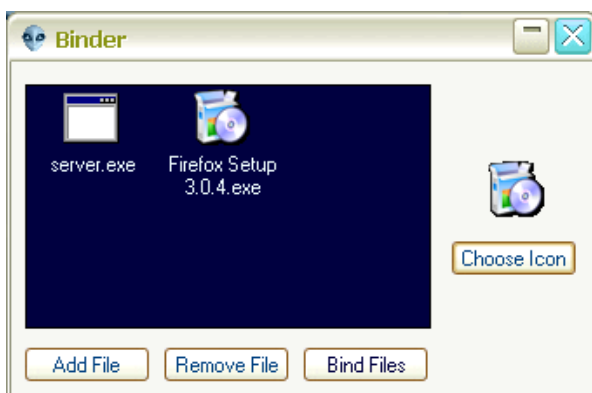
- Trong phần Server Setting, thiết lập các thông số trong các phần Basic, Notification, AV-FW Kill, ... và chọn Save Server:



- Tại giao diện Beast, ta chọn Binder



- Trong phần binder, Add Trojan và chương trình (cần nhúng – Firefox) vào, sau đó chọn Binder Files



Phân phối Trojan: → Chia sẻ các chương trình đã nhúng Trojan, cài chương trình Firefox đã làm ở trên vào máy Victim

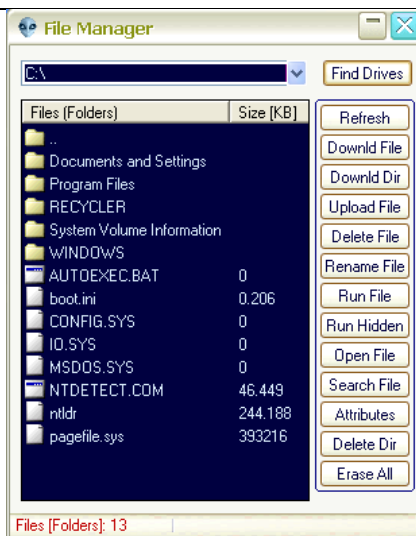
services.exe	SYSTEM	00	3,136 K
lsass.exe	SYSTEM	00	1,656 K
vmacthlp.exe	SYSTEM	00	2,320 K
svchost.exe	SYSTEM	00	4,596 K
svchost.exe	SYSTEM	00	20,868 K
spoolsv.exe	SYSTEM	00	5,416 K
hp4.exe	XP	03	472 K
VMwareTray.exe	XP	00	4,592 K
VMwareUser.exe	XP	00	7,688 K
Firefox Setup 3.0...	XP	00	2,384 K
setup.exe	XP	00	5,300 K
wuauclt.exe	XP	00	5,052 K
explorer.exe	XP	nn	16,240 K

Điều khiển Trojan:

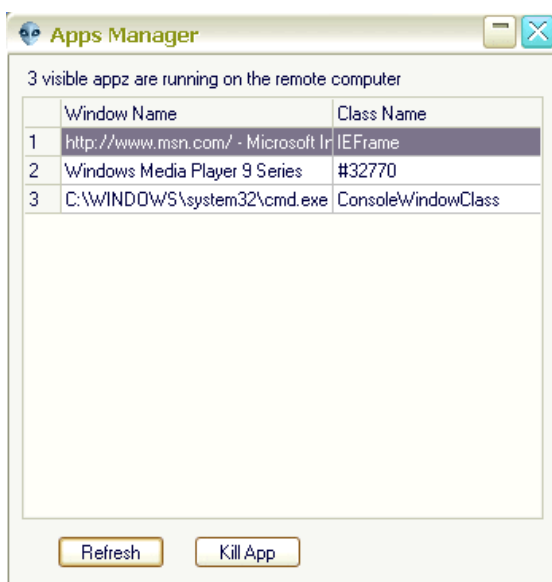
- Sử dụng Beast, kết nối đến Trojan trên máy Victim



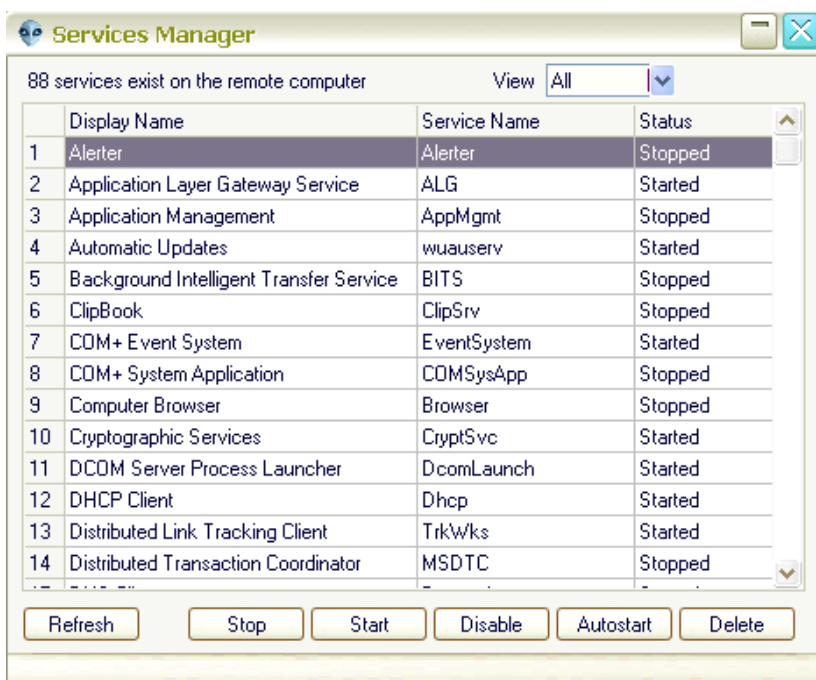
- Truy xuất file (hoặc thư mục trên máy Victim)
 - Tại phần giao diện Beast, chọn Managers → Files



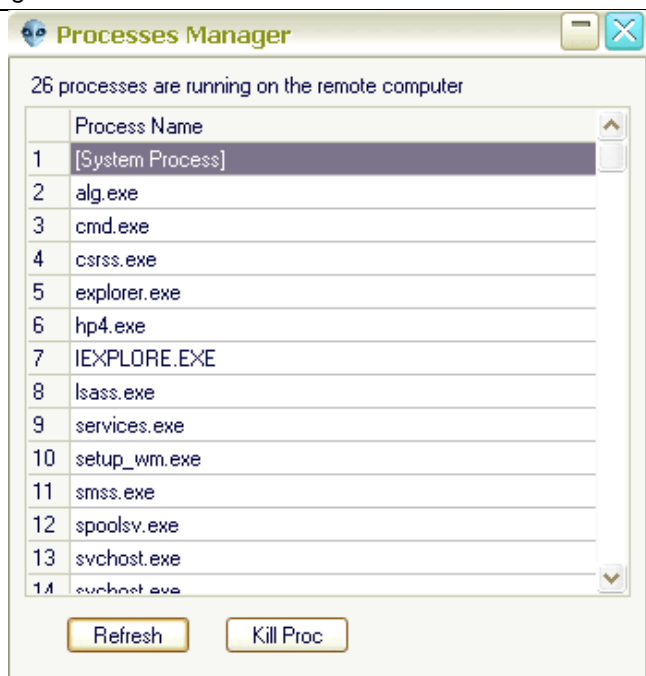
- Quản lý các ứng dụng, dịch vụ trên máy Victim
 - Tại phần giao diện Beast, chọn Managers → Apps (quản lý ứng dụng)



- Tại phần giao diện Beast, chọn Managers → Services (quản lý dịch vụ)



- Tại phần giao diện Beast, chọn Managers → Processes (quản lý tiến trình)



- Xem màn hình máy Victim
 - Tại phần giao diện Beast, chọn Managers → Screen



II. Các kỹ thuật xây dựng Worm:

II.1 Khái niệm Worm:

Sâu máy tính (worm) là một chương trình máy tính có khả năng tự nhân bản giống như virus máy tính.

Trong khi virus máy tính bám vào và trở thành một phần của mã máy tính để có thể thi hành thì sâu máy tính là một chương trình độc lập không nhất thiết phải là một phần của một chương trình máy tính khác để có thể lây nhiễm. Sâu máy tính thường được thiết kế để khai thác khả năng truyền thông tin có trên những máy tính có các đặc điểm chung - cùng hệ điều hành hoặc cùng chạy một phần mềm mạng - và được nối mạng với nhau.

II.2 Cơ chế Worm lây lan và phát tán:

Tất cả các virus không thể phát tán trừ khi bạn mở hoặc chạy 1 chương trình đang bị nhiễm virus.

Nhiều virus nguy hiểm nhất chủ yếu phát tán qua các tập tin đính kèm với thư điện tử – các tập tin gửi kèm với các tập tin điện tử.

CHƯƠNG 6

CÁC PHƯƠNG PHÁP PHÒNG CHỐNG

I. GIỚI THIỆU

CÁC NGUY CƠ

Theo thống kê của các hàng bảo mật mạng lớn trên thế giới thì tác hại, hậu quả do Virus máy tính gây ra đối với hệ thống mạng là rất lớn. Một số nguy cơ điển hình:

Làm giảm hiệu suất làm việc do virus gây ra làm tắc nghẽn băng thông mạng (Gửi email liên tục làm tắc nghẽn mạng, gửi các gói tin broadcast,..., chiếm dụng tài nguyên (CPU, RAM,...) của máy tính, làm giảm tốc độ máy, ... thậm chí có thể làm dừng hoạt động của cả một hệ thống mạng hoặc các máy chủ, máy trạm quan trọng. Nguy cơ này được đánh giá là gây ra mức thiệt hại lớn nhất.

Thay đổi, xóa nội dung dữ liệu. Mức độ thiệt hại của nguy cơ này phụ thuộc vào tầm quan trọng của dữ liệu bị sửa, xóa.

Đánh cắp dữ liệu, account. Virus máy tính có khả năng lấy cắp, ghi lại mật khẩu, username quan trọng, dữ liệu quan trọng rồi gửi đến địa chỉ của hacker.

Tạo các back-door. Việc virus máy tính tự động mở các cổng trên hệ thống không còn xa lạ, nó có thể mở cổng nhằm thực hiện các hành vi trái phép, gây nguy hiểm cho hệ thống hoặc sử dụng làm công cụ để tấn công làm hỏng hệ thống khác.

LỰA CHỌN GIẢI PHÁP

Một doanh nghiệp lớn với nhiều máy tính kết nối internet luôn cần một giải pháp phòng chống virus một cách hiệu quả nhất. Đối với các mạng doanh nghiệp này, việc xây dựng một hệ thống antivirus duy nhất cho cả một hệ thống máy tính, giúp người quản trị đơn giản hơn trong việc quản trị hệ thống, tiết kiệm băng thông, nâng cao bảo mật cho hệ thống.

Thông thường, một doanh nghiệp có kết nối internet, virus có thể thông qua một số con đường chính sau để lây nhiễm và tấn công vào hệ thống: thông qua việc truy cập internet; Email; việc truyền thông trong

mạng; các ứng dụng trên máy chủ, máy trạm; các thiết bị lưu trữ: CD, USB, HDD,...

Để bảo vệ phòng chống virus được hiệu quả cho hệ thống mạng trong toàn bộ doanh nghiệp, cần phòng chống virus trên tất cả các con đường mà virus có thể lây nhiễm, tấn công vào hệ thống. Cụ thể cần phòng chống virus cho: đường kết nối internet, Mail Server, luồng mail POP3 tại các máy trạm, các máy chủ,...

Phòng chống virus cho đường kết nối internet: Để phòng chống virus cho đường kết nối internet, cụ thể cần làm sạch virus cho các luồng HTTP, FTP, SMTP,... khi kết nối với môi trường internet, ta có thể sử dụng các sản phẩm web security và mail security. Ví dụ: Để phòng chống virus trên luồng HTTP và FTP có thể sử dụng sản phẩm Symantec Web Security. Để chống virus và lọc spam mail trên luồng SMTP có thể sử dụng sản phẩm Symantec Mail Security for SMTP.

Đối các luồng POP3 tại các máy trạm: Để phòng chống virus cho luồng mail POP3 thì cần phải sử dụng kết hợp với giải pháp phòng chống virus trên các máy trạm.

Phòng chống virus cho máy chủ: Để phòng chống virus cho các máy chủ thì trên máy chủ sử dụng các chương trình antivirus cho máy chủ. Hầu hết các sản phẩm antivirus đều có những đặc điểm sau:

- Quản trị theo mô hình tập trung: Điều này cho phép người quản trị từ một điểm có thể quản lý tất cả các máy được cài đặt chương trình antivirus.
- Quản trị từ xa theo mô hình đa lớp: Hầu hết các sản phẩm loại này đều cho phép quản trị từ xa thông qua kiến trúc đa lớp gồm các thành phần:
 - + Primary Server: Được cài trên một Server với mục đích quản lý tập trung các Secondary Server. Các chính sách về quản lý và cập nhật definition của virus sẽ được thiết lập trên máy Primary Server và sau đó được phân tán xuống các máy trạm thông qua các Secondary Server.
 - + Secondary Server: Được cài đặt trên các server được quản lý bởi Primary Server. Đây là thành phần quản lý trực tiếp các máy cần bảo vệ.
 - + Protected Machine: Đây là thành phần được bảo vệ trong hệ thống (máy tính của người dùng, các server)
 - + Management Console: Đây là công cụ quản trị, người quản trị có thể kết nối vào Primary Server để cấu hình và quản lý các máy trong hệ thống. Các chức năng quản lý từ xa có thể có: Update các definition, scan engine, scan virus, thiết

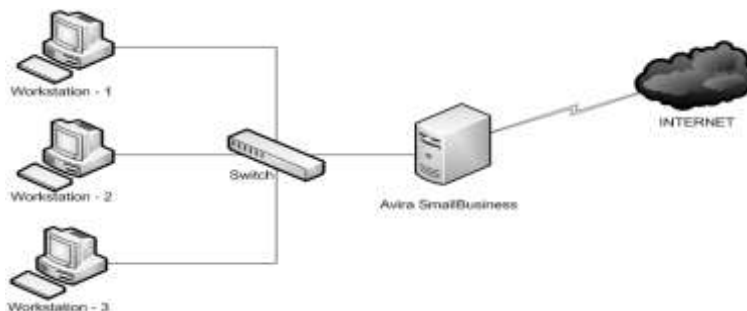
lập cấu hình scan virus cho các máy trong hệ thống, thiết lập cảnh báo, ghi nhật ký và báo cáo,...

Phòng chống virus cho các máy trạm: Để phòng chống virus cho các máy trạm trong hệ thống mạng doanh nghiệp cần sử dụng giải pháp antivirus cho các máy trạm trên môi trường mạng LAN được thiết kế theo mô hình client/server. Các sản phẩm loại này có những đặc điểm sau:

- Hoạt động theo mô hình Client-Server
- Hỗ trợ nhiều phương pháp triển khai chương trình antivirus cho các máy trạm
- Tự động cập nhật virus definition, scan engine. Các bản cập nhật được tải về máy chủ, sau đó các máy trạm truy cập vào để update, điều này giúp tiết kiệm băng thông internet
- Người quản trị có thể điều khiển từ xa quét virus, cập nhật virus definition cho các máy trạm
- Đặt lịch quét, cập nhật tự động

II. VÍ DỤ - TRIỂN KHAI AVIRA SMALLBUSINESS SUITE

MÔ HÌNH TRIỂN KHAI



YÊU CẦU SERVER

Hệ điều hành: Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Small Business Server, Windows Server 2003 x64 edition

YÊU CẦU CLIENT

Hệ điều hành: Windows XP Professional, Windows XP Professional x64 edition, Windows Vista 32 Bit, Windows Vista 64 Bit, Windows 7

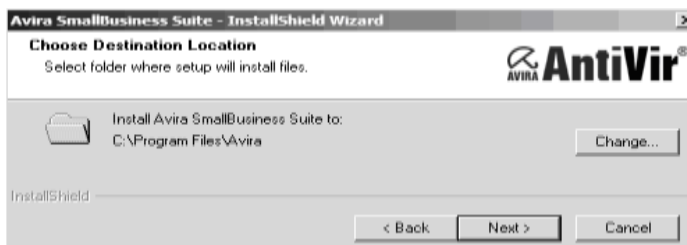
CÁC BƯỚC THỰC HIỆN

II.1.1 Cài đặt Avira SmallBusiness Suite:

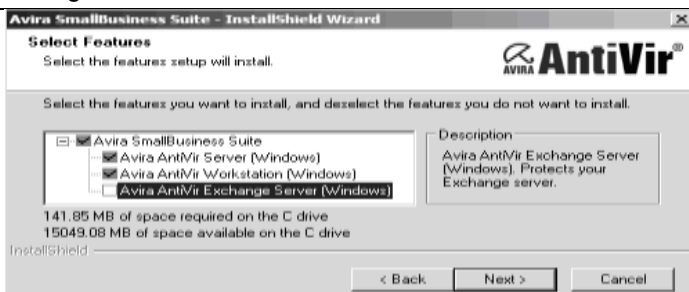
- Kích hoạt file cài đặt Avira SmallBusiness Suite, sau đó chọn Continue
- Tại màn hình Welcome to the InstallShield Wizard for Avira SmallBusiness Suite, chọn Next
- Tại màn hình License Agreement, check vào tùy chọn I accept the terms of the license agreement, sau đó chọn Next
- Tại màn hình Select License Key, chọn Browse chỉ đến Key tương ứng, sau đó chọn Next



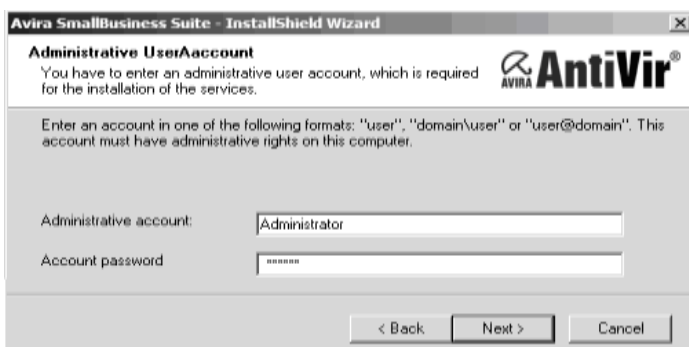
- Tại màn hình Choose Destination Location, chọn Next



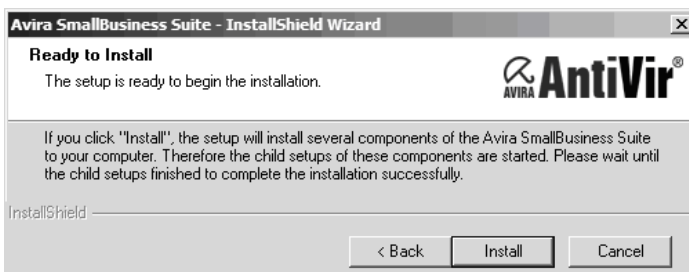
- Tại màn hình Select Features, chọn Next



- Tại màn hình Administrative UserAccount, nhập vào Username và password quản trị



- Tại màn hình Ready to Install, chọn Install



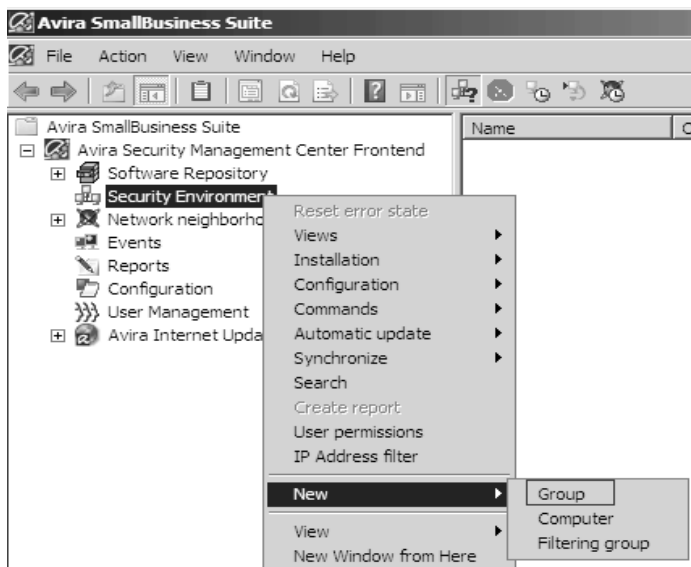
- Tại màn hình InstallShield Wizard Complete, chọn Finish

II.1.2 Quản trị Avira SmallBusiness Suite:

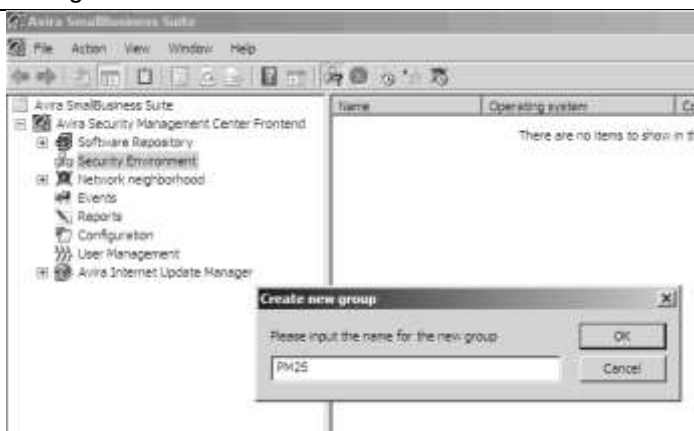
- Vào Start → Programs → Avira → Avira Security Management Center → Avira Security Management Center Frontend



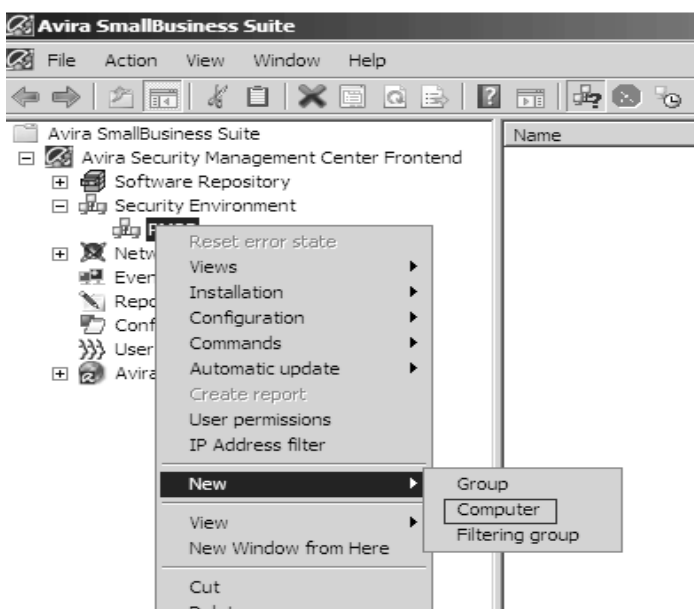
- Tạo mới một nhóm: Chọn Security Environment → Click phải chuột → New → Group



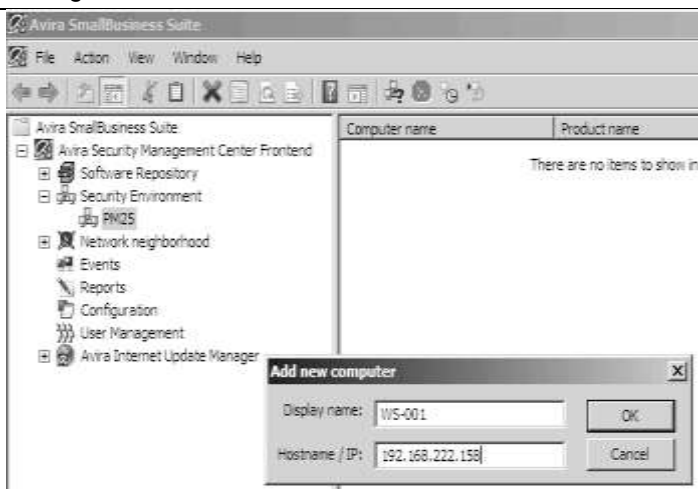
- Hộp thoại Create new group xuất hiện, nhập vào tên group cần khởi tạo, sau đó chọn OK



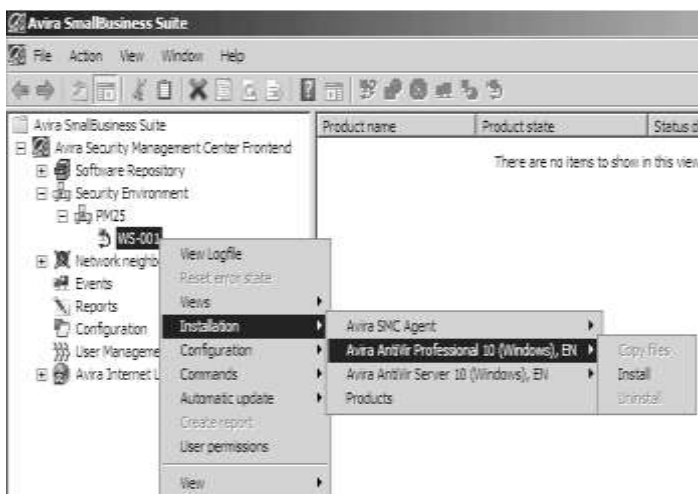
- Thêm một Computer vào nhóm: Click phải chuột lên nhóm cần thêm computer, chọn New → Computer



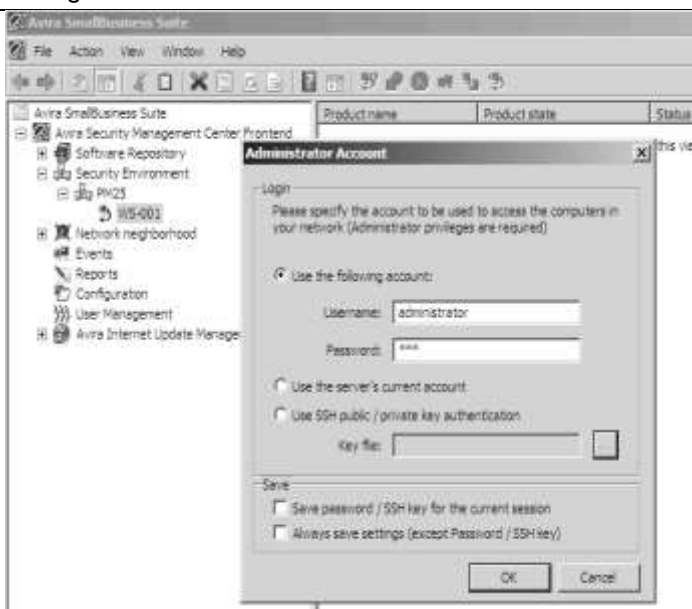
- Hộp thoại Add new computer xuất hiện, nhập vào Display name và Hostname/IP, sau đó chọn OK



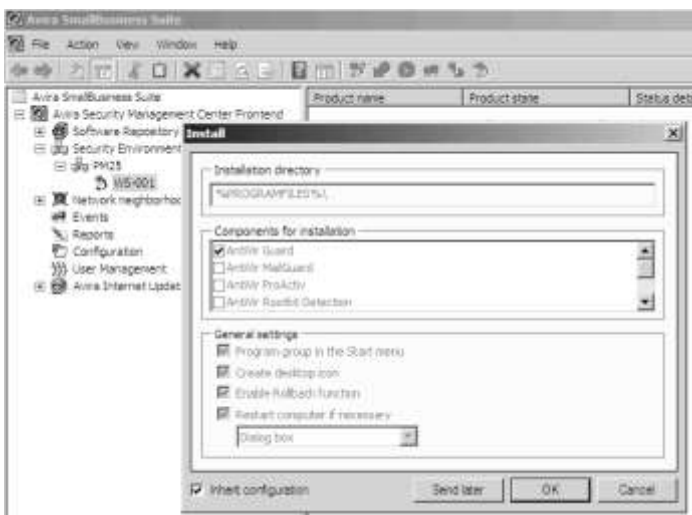
- Cài đặt Avira AntiVir Professional 10 cho computer: Click chuột phải vào computer cần cài đặt Avira AntiVir Professional 10, chọn Installation → Avira AntiVir Professional 10 (Windows), EN → Install



- Hộp thoại Administrator Account xuất hiện, nhập vào thông tin chứng thực với computer này

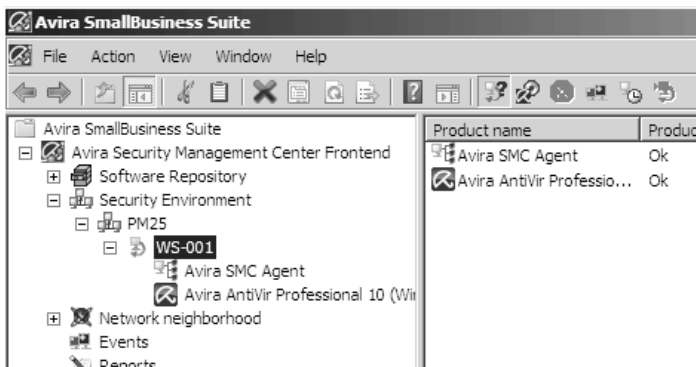


- Tại hộp thoại Install, chọn các components để cài đặt, sau đó chọn OK



- Khi Avira AntiVir Professional 10 đã cài xong:

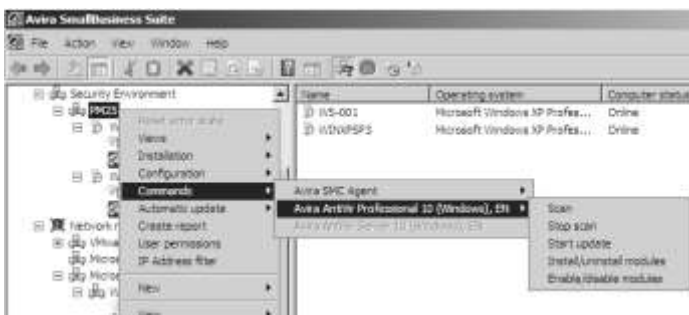
- Trên Avira Security Management Center Frontend:



- Trên máy WS-001



- Thực hiện các thao tác Start scan, Stop scan, Start update, install/uninstall modules, enable/disable modules



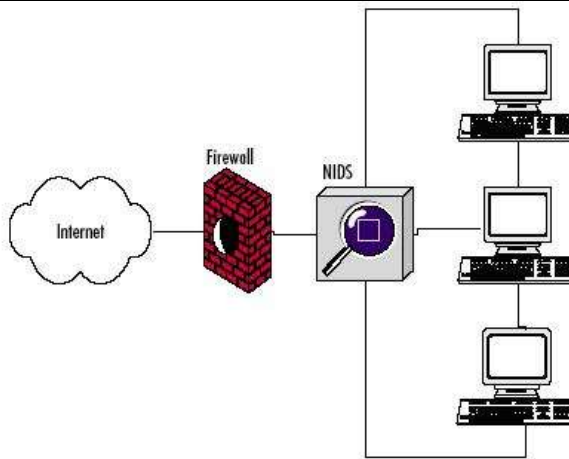
CHƯƠNG 7

CÁCH THỨC XÂY DỰNG HỆ THỐNG IDS/IPS

I. Hệ thống phát hiện xâm nhập – IDS

Đặc điểm chức năng và hoạt động :

- Là hệ thống theo dõi và phát hiện đột nhập.
- Bằng cách theo dõi các hoạt động diễn ra trên mạng hay trên một máy tính và so sánh với những thông tin đã biết, IDS có thể phát hiện các hành động thâm nhập hay tấn công, khi đó sẽ phát tín hiệu báo động và ghi log để làm tài liệu cho việc khắc phục sau này.
- Việc cập nhật các dấu hiệu tấn công là công việc khó nhất trong kỹ thuật IDS. Dấu hiệu tấn công có thể xây dựng từ các đặc điểm như IP option, một mẫu (pattern) của dữ liệu di chuyển trên mạng hay tần số lặp đi lặp lại một đặc điểm của phương pháp tấn công nào đó ...
- Có hai loại IDS có thể dùng trong việc tăng cường tính bảo mật. System IDS cài đặt để hoạt động trên các server và network IDS (NIDS) hoạt động phát hiện đột nhập trên mạng. System IDS thường hiệu quả hơn NIDS tuy nhiên NIDS sẽ hiệu quả trong các trường hợp như tấn công vào nhiều server cùng một lúc hay các đợt quét port của attacker mà system IDS không thể phát hiện.
- IDS không chỉ là biện pháp phòng thủ thụ động. Một số hệ thống IDS có khả năng ứng phó như kết hợp với firewall để chặn IP nào đó. IDS có thể cấu hình để bổ sung các dấu hiệu tấn công. Một vài NIDS có thể cấu hình ở chế độ learning mode, khi đó NIDS sẽ đề nghị hoặc tự động điều chỉnh các cấu hình cho phù hợp với mạng qua quá trình theo dõi và tổng hợp lưu thông.



System IDS được cài đặt trên các server (trên một máy tính nhất định) trong khi NIDS cài đặt sao cho có thể theo dõi toàn bộ mạng.

Điểm yếu bảo mật :

- Điểm yếu của NIDS là có thể bị quá tải. Khi lưu lượng truyền thông trên mạng lớn, NIDS không thể nào kiểm tra từng packet một. Khi đó khả năng bỏ sót packet sẽ xảy ra và đó là điều mà attacker mong muốn.

Các điểm cần để ý khi triển khai NIDS :

- Đảm bảo NIDS phù hợp với kích thước mạng. Nếu NIDS không đáp ứng nổi chúng ta nên thay NIDS mới hoặc chia nhỏ mạng để có thể theo dõi với nhiều NIDS.
- Khi cấu hình NIDS từ xa tốt nhất nên thực hiện từ một máy tính nằm khác subnet.
- Thực hiện ghi log lên một máy tính khác nằm khác subnet với NIDS để tăng tính bảo mật.

II. Hệ thống ngăn ngừa xâm nhập IPS

Hai kiểu IPS được biết trên thị trường hiện nay là “dựa vào máy chủ” và “nội tuyến” (dựa vào mạng). Các hệ thống “dựa vào máy chủ” là các phần mềm ngăn ngừa xâm nhập được viết để “móc” trực tiếp vào trong các ứng dụng hay cài đặt trực tiếp trên các máy chủ ứng dụng. Bài viết này chỉ tập trung vào bảo mật “nội tuyến”. Bảo mật “nội tuyến” tương tự như trong kiến trúc tường lửa di trú kép hay một cổng chống vi rút được đặt ngược chiều từ các ứng dụng được bảo vệ và áp dụng các

dịch vụ ngăn ngừa xâm nhập cho nhiều ứng dụng xuôi chiều của các IPS.

Theo đúng nghĩa của khái niệm này, ta có thể định nghĩa như sau: “Một Hệ thống Ngăn ngừa Xâm nhập “nội tuyến” (inline) là bất kỳ một thiết bị phần cứng hay phần mềm nào có khả năng phát hiện và ngăn ngừa các cuộc tấn công đã quen biết”. Thậm chí đơn giản hơn, “Ngăn ngừa Xâm nhập” chỉ đề cập đến việc phát hiện và sau đó ngăn chặn những cuộc tấn công chuyên biệt ứng dụng đã biết. Thuật ngữ “Hệ thống Ngăn ngừa Xâm nhập” (Intrusion Prevention System) bản thân được sử dụng để hợp nhất cả hai khái niệm “Hệ thống Phát hiện” (detection system) và “Hệ thống Ngăn ngừa” (prevention system) dưới một cấu trúc.

Phát hiện và ngăn ngừa

Nhìn bề ngoài, các giải pháp phát hiện xâm nhập và ngăn ngừa xâm nhập xuất hiện theo kiểu cạnh tranh nhau. Rốt cuộc, chúng chia sẻ một danh sách các chức năng giống nhau như kiểm tra gói tin, phân tích có trạng thái, ráp lại các đoạn, ráp lại các TCP-segment, kiểm tra gói tin sâu, xác nhận tính hợp lệ giao thức và thích ứng chữ ký. Một IPS hoạt động giống như một người bảo vệ gác cổng cho một khu dân cư, cho phép và từ chối truy nhập dựa trên cơ sở các uỷ nhiệm và tập quy tắc nội quy nào đó. Một IDS (hệ thống phát hiện xâm nhập) làm việc giống như một xe tuần tra bên trong khu dân cư, giám sát các hoạt động và tìm ra những tình huống bất bình thường. Dù mức độ an ninh tại cổng vào khu dân cư mạnh đến mức nào, xe tuần tra vẫn tiếp tục hoạt động trong một hệ thống giám sát và sự cân bằng của chính nó.

Phát hiện xâm nhập

Mục đích của “phát hiện xâm nhập” là cung cấp sự giám sát, kiểm tra, tính pháp lý và báo cáo về các hoạt động của mạng. Nó hoạt động trên các gói tin được cho phép thông qua một thiết bị kiểm soát truy nhập. Do những hạn chế về độ tin cậy và những đe dọa bên trong, “Ngăn ngừa Xâm nhập” phải cho phép một số “vùng xám” (gray area) tấn công để tránh các trường hợp báo động giả. Mặt khác, những giải pháp IDS được “nhồi” trí thông minh có sử dụng nhiều kỹ thuật khác nhau để nhận biết những cuộc xâm nhập, những khai thác, lạm dụng bất chính và các cuộc tấn công tiềm tàng. Một IDS có thể thực hiện các hoạt động mà không làm ảnh hưởng đến các kiến trúc tính toán và kết nối mạng.

Bản chất bị động của IDS nằm ở chỗ cung cấp sức mạnh để chỉ đạo phân tích thông minh các lưu lượng gói tin. Những vị trí IDS này có thể nhận ra :

- Các cuộc tấn công quen biết theo đường chữ ký (signature) và các quy tắc.
- Những biến thiên trong lưu lượng và phương hướng sử dụng những quy tắc và phân tích thống kê phức tạp.
- Những biến đổi mẫu lưu lượng truyền thông có sử dụng phân tích luồng.
- Phát hiện hoạt động bất bình thường có sử dụng phân tích độ lệch đường cơ sở (baseline deviation analysis).
- Phát hiện hoạt động đáng nghi nhờ phân tích luồng, các kỹ thuật thống kê và phát hiện sự bất bình thường.

Ngăn ngừa xâm nhập

Như được đề cập trước đây, các giải pháp “Ngăn ngừa Xâm nhập” nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe dọa tấn công bằng việc loại bỏ những lưu lượng mạng có hại hay có ác ý trong khi vẫn cho phép các hoạt động hợp pháp tiếp tục. Mục đích ở đây là một hệ thống hoàn hảo – không có những báo động giả nào làm giảm năng suất người dùng cuối và không có những từ chối sai nào tạo ra rủi ro quá mức bên trong môi trường. Có lẽ một vai trò cốt yếu hơn sẽ là cần thiết để tin tưởng, để thực hiện theo cách mong muốn dưới bất kỳ điều kiện nào. Điều này có nghĩa các giải pháp “Ngăn ngừa Xâm nhập” được đặt vào đúng vị trí để phục vụ với:

- Những ứng dụng không mong muốn và những cuộc tấn công “Trojan horse” nhằm vào các mạng và các ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và các danh sách điều khiển truy nhập (access control lists).
- Các gói tin tấn công giống như những gói tin từ LAND và WinNuke qua việc sử dụng các bộ lọc gói tốc độ cao.
- Sự lạm dụng giao thức và những hành động lảng tránh – những thao tác giao thức mạng giống như Fragroute và những khảo sát lán TCP (TCP overlap exploits) – thông qua sự ráp lại thông minh.
- Các tấn công từ chối dịch vụ (DOS/DDOS) như “lụt” các gói tin SYN và ICMP bởi việc sử dụng các thuật toán lọc dựa trên cơ sở ngưỡng.

- Sự lạm dụng các ứng dụng và những thao tác giao thức – các cuộc tấn công đã biết và chưa biết chống lại HTTP, FTP, DNS, SMTP .v.v. – qua việc sử dụng những quy tắc giao thức ứng dụng và chữ ký.
- Những cuộc tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng các hữu hạn tiêu thụ tài nguyên dựa trên cơ sở ngưỡng.
- Tất cả các cuộc tấn công và trạng thái dễ bị tấn công cho phép chúng tình cờ xảy ra đều được chứng minh bằng tài liệu. Ngoài ra, những khác thường trong các giao thức truyền thông từ mạng qua lớp ứng dụng không có chỗ cho bất cứ loại lưu lượng hợp pháp nào, làm cho các lỗi trở thành tự chọn lọc trong ngữ cảnh xác định.

Tình trạng của công nghệ IPS

Trạng thái của công nghệ IPS là chưa chín muồi nếu bạn xem xét ở góc độ sản phẩm của từng nhà cung cấp đơn lẻ với tất cả các tính năng phát hiện, giám sát, ngăn ngừa, cập nhật và báo cáo trên mỗi sự truyền tải cho truy nhập vào trong và ra ngoài qua một điểm nghẽn (choke-point) mạng đặc biệt. Gần đây, các doanh nghiệp đã tiêu tốn hàng triệu đô la vào các sản phẩm để giúp đỡ họ bảo vệ an toàn mạng của họ. Các sản phẩm IPS mới nổi của ngày nay được tập trung chủ yếu dành riêng cho Port 80 và như vậy chúng hiện không thay thế các hệ thống hiện tại.

Thay vào đó chúng làm tăng thêm giá trị của những hệ thống này. Một giải pháp IPS đa giao thức bao hàm tất cả sẽ phải được phát triển và chứng tỏ trước khi những hệ thống như vậy được coi như những thay thế thực tế cho các hệ thống đã triển khai.

Các mục tiêu dài hạn

Trong tương lai, một giải pháp cổng an ninh nội tuyến (inline) phải đạt được các mục tiêu này :

- Khả năng phát hiện và ngăn chặn tấn công dựa trên cơ sở sử dụng logic và vật lý của nhiều công nghệ ép buộc. Rộng hơn, điều này còn bao gồm cả khả năng ngăn ngừa cả hai dạng tấn công đã biết và chưa biết có sử dụng các biện pháp phòng thủ ứng dụng (Application Defenses).
- Khả năng cùng nhau hoạt động với cơ sở hạ tầng an ninh được triển khai cho những mục đích hỗ trợ tập hợp dữ liệu,

bằng chứng điện tử, giám sát theo dõi và phục tùng điều chỉnh khi cần.

- Khả năng không phá vỡ những hoạt động kinh doanh do thiếu tính sẵn sàng, hiệu năng kém, những khẳng định sai hay không có khả năng hoạt động cùng nhau với các cơ sở hạ tầng chứng thực quy định.
- Khả năng hỗ trợ các chuyên gia an ninh CNTT trong việc chuyển giao kế hoạch quản lý rủi ro của tổ chức của họ bao gồm chi phí cho thực hiện, hoạt động và những kết quả làm việc từ các cảnh báo và báo cáo từ hệ thống.

Những thách thức để đạt được mục đích

Hiện thời không có các nghiên cứu của đối tác thứ ba có thể chấp nhận được tính hiệu quả của IPS như là một giải pháp. Sự quảng cáo thổi phồng xung quanh “Ngăn ngừa Xâm nhập” đang làm lẫn lộn giữa những gì công nghệ này có thể cung cấp và những gì nó hứa hẹn.

Cách tiếp cận nhiều lớp cho an ninh CNTT tiếp tục có giá trị trong khi công nghiệp phát triển. Nó không có vẻ là sự di trú ra xa khỏi phòng thủ chiều sâu phân lớp đúng như nó được tổ chức.

Nhiều giải pháp IPS sẽ đòi hỏi những yêu cầu giống IDS để điều chỉnh, giám sát và báo cáo.

Mục Lục

CHƯƠNG 1	1
GIỚI THIỆU TỔNG QUAN AN NINH MẠNG	1
I. ĐIỀU KHIỂN TRUY CẬP	1
MAC (MANDATORY ACCESS CONTROL)	1
DAC (DISCRETIONARY ACCESS CONTROL)	2
RBAC (ROLE-BASED ACCESS CONTROL)	2
II. XÁC THỰC.....	2
USERNAME/PASSWORD	2
KERBEROS	3
CHAP	4
CHỨNG CHỈ (CERTIFICATES)	5
MUTUAL AUTHENTICATION	6
BIOSMETRICS	6
MULTI-FACTOR.....	8
III. KIỂM TOÁN (AUDITING)	9
AUDITING SYSTEM.....	9
CHƯƠNG 2	11
CÁC HÌNH THỨC.....	11
TẤN CÔNG MẠNG PHỔ BIẾN	11
I. MINH HỌA KHÁI QUÁT MỘT KỊCH BẢN TẤN CÔNG	11
II. TẤN CÔNG CHỦ ĐỘNG.....	12
DOS	12
DDoS	13
BUFFER OVERFLOWS	14
SYN ATTACKS	14
SPOOFING	16
MAN IN THE MIDDLE ATTACKS	17
RELAY ATTACKS	18
DUMPSTER DIVING	18
SOCIAL ENGINEERING	18
III. TẤN CÔNG THỤ ĐỘNG.....	18

DÒ TÌM LỖ HỔNG(VULNERABILITY SCANNING)	18
GIỚI THIỆU MỘT SỐ CÔNG CỤ DÒ TÌM LỖ HỔNG:	19
NGHE LÉN(SNIFFING).....	21
PASSWORD ATTACKS	25
MALICIOUS CODE ATTACK	25
CHƯƠNG 3	27
KỸ THUẬT KHAI THÁC WEBSITE	27
I. BẢO MẬT WEB.....	27
BẢO MẬT TRÊN WEB SERVER.....	27
BẢO MẬT TRÊN WEB CLIENT	29
GIAO THỨC SSL VÀ HTTPS	30
CÁC LỖ HỔNG BẢO MẬT LIÊN QUAN ĐẾN WEB VÀ CÁCH PHÒNG CHỐNG	46
CHƯƠNG 4	48
CÁC KỸ THUẬT KHAI THÁC LỖ HỔNG MẠNG KHÔNG DÂY	48
I. BẢO MẬT TRÊN HỆ THỐNG MẠNG KHÔNG DÂY	48
GIỚI THIỆU	48
CÁC CHUẨN BẢO MẬT TRÊN HỆ THỐNG MẠNG KHÔNG DÂY	48
CHƯƠNG 5	50
CÁC KỸ THUẬT SỬ DỤNG TROJAN, WORM	50
I. KỸ THUẬT SỬ DỤNG TROJAN:	50
I.1 KHÁI NIỆM TROJAN:	50
I.2 MÔ HÌNH TRIỂN KHAI.....	50
II. CÁC KỸ THUẬT XÂY DỰNG WORM:	58
II.1 KHÁI NIỆM WORM:.....	58
II.2 CƠ CHẾ WORM LÂY LAN VÀ PHÁT TÁN:	58
CHƯƠNG 6	60
CÁC PHƯƠNG PHÁP	60
PHÒNG CHỐNG	60
I. GIỚI THIỆU	60
CÁC NGUY CƠ.....	60

LỰA CHỌN GIẢI PHÁP	60
II. VÍ DỤ - TRIỂN KHAI AVIRA SMALLBUSSINESS SUITE	62
MÔ HÌNH TRIỂN KHAI	62
YÊU CẦU SERVER	62
YÊU CẦU CLIENT	62
CÁC BƯỚC THỰC HIỆN	63
II.1.1 CÀI ĐẶT AVIRA SMALLBUSSINESS SUITE:	63
II.1.2 QUẢN TRỊ AVIRA SMALLBUSINESS SUITE:.....	64
CHƯƠNG 7	70
CÁCH THỨC XÂY DỰNG.....	70
HỆ THỐNG IDS/IPS	70
I. HỆ THỐNG PHÁT HIỆN XÂM NHẬP – IDS	70
II. HỆ THỐNG NGĂN NGỪA XÂM NHẬP IPS.....	71
PHÁT HIỆN VÀ NGĂN NGỪA.....	72
PHÁT HIỆN XÂM NHẬP.....	72
NGĂN NGỪA XÂM NHẬP.....	73
TÌNH TRẠNG CỦA CÔNG NGHỆ IPS	74
CÁC MỤC TIÊU DÀI HẠN	74
NHỮNG THÁCH THỨC ĐỂ ĐẠT ĐƯỢC MỤC ĐÍCH	75
MỤC LỤC	76