**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
Khoa Mạng máy tính và Truyền thông**

**🙢 🕮 🙠**

**Bài Tập Nhóm**

**Môn:**

**AN TOÀN MẠNG MÁY TÍNH**

**Giáo viên hướng dẫn: Tô Nguyễn Nhật Quang**

**Nhóm sinh viên thực hiện :**

***TRẦN HỮU TIẾN 13521072***

***NGUYỄN ĐẶNG THẮNG***

**Thành phố Hồ Chí Minh - tháng 5/2015**

# Lời cảm ơn

Trên thực tế không có sự thành công nào mà không gắn liền với những sự hỗ trợ, giúp đỡ dù ít hay nhiều, dù trực tiếp hay gián tiếp của người khác. Trong suốt thời gian từ khi bắt đầu học tập ở giảng đường đại học đến nay, em đã nhận được rất nhiều sự quan tâm, giúp đỡ của quý Thầy Cô, gia đình và bạn bè.

Với lòng biết ơn sâu sắc nhất, em xin gửi đến quý Thầy Cô ở Khoa Khoa Mạng Máy Tính và Truyền Thông – Trường Đại Học Công Nghệ Thông Tin đã cùng với tri thức và tâm huyết của mình để truyền đạt vốn kiến thức quý báu cho chúng em trong suốt thời gian học tập tại trường. Và đặc biệt, trong học kỳ này, Khoa đã tổ chức cho chúng em được tiếp cận với môn học mà theo em là rất hữu ích đối với sinh viên ngành Mạng Máy Tính cũng như tất cả các sinh viên thuộc các chuyên ngành Khoa Mạng Máy Tính và Truyền Thông khác. Đó là môn học “An Toàn Mạng Máy Tính”.

Em xin chân thành cảm ơn đã tận tâm Tô Nguyễn Nhật Quang đã hướng dẫn chúng em qua từng buổi học trên lớp cũng như những buổi nói chuyện, thảo luận về lĩnh vực sáng tạo trong nghiên cứu khoa học. Nếu không có những lời hướng dẫn, dạy bảo của thầy thì em nghĩ bài thu hoạchnày của em rất khó có thể hoàn thiện được. Một lần nữa, em xin chân thành cảm ơn thầy.

Bài thu hoạch được thực hiện trong khoảng thời gian gần 8 tuần. Bước đầu đi vào thực tế, tìm hiểu về lĩnh vực sáng tạo trong nghiên cứu khoa học, kiến thức của em còn hạn chế và còn nhiều bỡ ngỡ. Do vậy, không tránh khỏi những thiếu sót là điều chắc chắn, em rất mong nhận được những ý kiến đóng góp quý báu của quý Thầy Cô và các bạn học cùng lớp để kiến thức của em trong lĩnh vực này được hoàn thiện hơn.

MỤC LỤC

[Lời cảm ơn 1](#_Toc436958848)

[1 Hợp Đồng Nhóm 5](#_Toc436958849)

[1.1 Thành viên 5](#_Toc436958850)

[1.2 Mục tiêu đề ra 5](#_Toc436958851)

[1.3 Quy tắc 5](#_Toc436958852)

[1.4 Bảng phân công công việc 6](#_Toc436958853)

[1.5 Đánh giá 7](#_Toc436958854)

[1.6 Cam kết 7](#_Toc436958855)

[Dựa trên hợp đồng nhóm đã đưa ra, chúng tôi cam kết sẽ hoàn thành đúng yêu cầu trên. 7](#_Toc436958856)

[Hồ Chí Minh, Ngày…Tháng…Năm… 7](#_Toc436958857)

[Thành viên 1 Thành viên 2 Thành viên 3 Thành viên 4 7](#_Toc436958858)

[( kí tên ) ( kí tên ) ( kí tên ) ( kí tên ) 7](#_Toc436958859)

[2 Chương 1 8](#_Toc436958860)

[2.1 Firewall 8](#_Toc436958861)

[**2.1.1** **Khái niệm** 8](#_Toc436958862)

[**2.1.2** **Lịch sử** 8](#_Toc436958863)

[**2.1.3** **Lý do sử dụng Firewall** 9](#_Toc436958864)

[**2.1.4** **Các loại Fireware** 9](#_Toc436958865)

[**2.1.5** **Nhiệm vụ.** 10](#_Toc436958866)

[**2.1.6** **Chức năng chính của Firewall** 10](#_Toc436958867)

[**2.1.7** **Firewall bảo vệ và chống lại cái gì?** 10](#_Toc436958868)

[**2.1.8** **Các thành phần cơ bản của Firewall và cơ chế hoạt động** 11](#_Toc436958869)

[**2.1.9** **Thuận lợi và hạn chế của Firewall** 13](#_Toc436958870)

[**2.1.10** **Kết luận** 14](#_Toc436958871)

[2.2 Các thuật toán mã hóa 15](#_Toc436958872)

[**2.2.1** **Phương thức mã hóa RSA** 15](#_Toc436958873)

[Là phương thức mã hóa công khai. Do Ron Rivest, Adi Shamir và Len Adleman tại học viên MIT đề xuất năm 1977. Và hiện nay đang được sử dụng rộng rãi. 15](#_Toc436958874)

[**2.2.2** **Phương thức mã hóa DES** 17](#_Toc436958875)

[**2.2.3** **Thuật toán mã hóa AES** 19](#_Toc436958876)

[2.3 VNP (virtual private network) 21](#_Toc436958877)

[**2.3.1** **Đặt vấn đề** 21](#_Toc436958878)

[**2.3.2** **VPN giới thiệu** 21](#_Toc436958879)

[**2.3.3** **Tính bảo mật của VNP** 23](#_Toc436958880)

[**2.3.4** **Các kĩ thuật sử dụng trong VNP** 24](#_Toc436958881)

[**2.3.5** **Kết luận** 25](#_Toc436958882)

[3 Một số phương pháp tấn công và cách phòng tránh 25](#_Toc436958883)

[3.1 Sniff (Nghe lén) 25](#_Toc436958884)

[**3.1.1** **Khái niệm** 25](#_Toc436958885)

[**3.1.2** **Sơ lược về cách tấn công** 26](#_Toc436958886)

[**3.1.3** **Các loại sniff và cơ chế hoạt động** 26](#_Toc436958887)

[**3.1.4** **Cách phát hiện và phòng chống** 27](#_Toc436958888)

[**3.1.5** **Mức độ ảnh hưởng đến hệ thống** 29](#_Toc436958889)

[3.2 Phishing 29](#_Toc436958890)

[**3.2.1** **Khái niệm** 29](#_Toc436958891)

[**3.2.2** **Thời gian xuất hiện** 29](#_Toc436958892)

[**3.2.3** **Sơ lược cách tấn công** 30](#_Toc436958893)

[**3.2.4** **Cách phòng chống** 30](#_Toc436958894)

[**3.2.5** **Mức độ ảnh hưởng** 31](#_Toc436958895)

[3.3 SQL Injection 32](#_Toc436958896)

[**3.3.1** **Khái niệm** 32](#_Toc436958897)

[**3.3.2** **Thời gian xuất hiện.** 32](#_Toc436958898)

[**3.3.3** **Cách thức tấn công** 32](#_Toc436958899)

[**3.3.4** **Kỹ thuật an ninh dùng để phòng chống SQL Injection** 36](#_Toc436958900)

[**3.3.5** **Mức độ ảnh hưởng** 37](#_Toc436958901)

[3.4 Tấn công từ chối dịch vị (DDoS) 38](#_Toc436958902)

[**3.4.1** **Khái niệm** 38](#_Toc436958903)

[**3.4.2** **Thời gian xuất hiện** 38](#_Toc436958904)

[**3.4.3** **Các cách tấn công** 38](#_Toc436958905)

[**3.4.4** **Cách thức phòng chống:** 41](#_Toc436958906)

[**3.4.5** **Mức độ ảnh hưởng:** 41](#_Toc436958907)

**LỜI NÓI ĐẦU**

Sự phát triển của mạng máy tính trong thập niên vừa qua rất nhanh chóng, từ những nhóm người dùng chung một mạng để chia sẽ tập tin, trao đổi thông tin một cách dễ dàng hơn cho đến những hệ thống mạng của một doanh nghiệp hay một tập đoàn lớn nhằm tăng hiệu quả về thời gian và kinh tế, tất cả đều nhờ đến mạng máy tính. Chính vì sự phổ biến và quan trọng đó đã có không ít kẻ xấu nhằm lợi dụng lỗ hổng bảo mật của các hệ thống mạng máy tính đó để nhằm xâm nhập hệ thống với quyền quản trị để lấy đi những thông tin quan trọng nhằm mục đích xấu. Đã có nhiều cách tấn công vào mạng, hệ thống khác nhau, được ra đời ở nhiều nơi trên thế giới, những cuộc tấn công như vậy thường gây thiệt hại về mặt kinh tế rất lớn, và tất nhiên những chuyên gia về mạng hệ thống củng đã tìm được những cách khắc phục để hạn chế tối đa tổn thất đó. Trên thực tế đó, hôm nay, nhóm chúng tôi xin trình bày những bài tập của giáo viên bộ môn đưa ra và dần dần áp dụng vào thực tế. Trong đề tài mà chúng tôi thự hiện vẫn còn một số thiếu sót mong mọi người bỏ qua cho. Xin cảm ơn!

# Hợp Đồng Nhóm

## Thành viên

|  |  |
| --- | --- |
| **Họ và Tên** | **MSSV** |
| Trần Hữu Tiến | 13521072 |
| Nguyễn Đặng Thắng |  |
|  |  |

## Mục tiêu đề ra

* Hoàn thành tốt những bài tập được thầy giao.
* Giúp đỡ nhau trong công việc.
* Rèn luyện khả năng làm việc nhóm.
* Hoàn thành học phần một cách xuất sắc nhất.
* Chia sẻ những kinh nghiệm quý giá trong quá trình tìm hiểu của mình cho các bạn trong nhóm.

## Quy tắc

* Làm việc trên cơ sở đồng thuận về ý kiến quan điểm chung.
* Tôn trọng ý kiến cá nhân của các thành viên nếu nó vẫn đảm bảo yêu cầu của công việc.
* Hoàn thành công việc đúng thời hạn.
* Giúp đỡ lẫn nhau khi có khó khăn.
* Ai không hoàn thành thì sẽ phải chịu trách nhiệm về công việc của mình.

## Bảng phân công công việc

|  |  |  |  |
| --- | --- | --- | --- |
| **Mã số sinh viên** | **Thành viên** | **Vai trò** | **Công việc** |
| 13521072 | Trần Hữu Tiến | Member | * Giới thiệu một số phương pháp tấn công và cách phòng tránh. * Thiết kế đồ án. * Đăng kí và nộp đồ án. |
| 13521038 | Hoàng Thế Vinh | Member | * Tìm hiểu về Firewall. * Kiểm tra và chỉnh sửa đồ án. |
| 13520973 | Nguyễn Công Thành Tú | Member | * Tìm hiểu về kỹ thuật mã hóa RSA. * Kiểm tra và chỉnh sửa đồ án. |
| 13520746 | Nguyễn Văn Tân | Member | * Tìm hiểu về VPN. * Kiểm tra và chỉnh sửa đồ án. * Tìm hiểu kỹ thuật tấn công DDoS |

## Đánh giá

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MSSV** | **Họ Tên** | **Tỷ lệ công việc được giao (%)** | **Tỷ lệ công việc hoàn thành (%)** | **Nhận xét**  **Trọng số điểm** |
| 13521072 | Trần Hữu Tiến | 25% | 95% | Tích cực trong công việc, hoành thành đúng thời hạn. 4.5 điểm |
| 13521038 | Hoàng Thế Vinh | 25% | 95% | Tích cực trong công việc.Nắm bắt nhanh thông tin cho nhóm. 4.5 điểm |
| 13520973 | Nguyễn Công Thành Tú | 25% | 95% | Có tinh thần, luôn tạo động lực làm việc cho nhóm. 4.5 điểm |
| 13520746 | Nguyễn Văn Tân | 25% | 95% | Hoàn thành công việc tốt, hòa nhã, tạo không khí làm việc nhóm. 4.5 điểm |

## Cam kết

## Dựa trên hợp đồng nhóm đã đưa ra, chúng tôi cam kết sẽ hoàn thành đúng yêu cầu trên.

Hồ Chí Minh, Ngày…Tháng…Năm…

Thành viên 1 Thành viên 2 Thành viên 3 Thành viên 4

( kí tên ) ( kí tên ) ( kí tên ) ( kí tên )

Chương 1

## Firewall

### **Khái niệm**

Trong ngành mạng máy tính, firewall (bức tường lửa) là rào chắn bảo vệ thiết bị phần cứng hoặc phần mềm hoạt động trong môi trường máy tính nối mạng mà một số các nhân, tổ chức, doanh nghiệp, cơ quan lập ra nhằm ngăn chặn người dùng internet truy cập các thông tin không mong muốn hoặc chặn người bên trong truy cập các thông tin bảo mật trong mạng nội bộ.

### **Lịch sử**

Ý tưởng được hình thành sau khi sảy ra hàng loạt cuộc tấn công vào cuối những năm 1980. Cuộc tấn công đầu tiên mang tính hệ thống máy tính là cuộc tấn công “Sâu Morris” được phát tán qua thư điện tử, nó gây ra tổn thất nghiêm trọng đối với hệ thống mạng. Từ đó cộng đồng Internet đã quyết định rằng ưu tiên tối cao là ngăn chặn không cho một cuộc tấn công mới sảy ra, họ bắt đầu đưa ra các ý tưởng mới, những hệ thống và phần mềm mới để làm cho mạng Internet trở nên an toàn hơn.

Năm 1988, bài báo đầu tiên về công nghệ tường lửa được công bố, khi Jeff Mogul thuộc Digital Equipment Corp phát triển các hệ thống lọc đầu tiên được biết đến với tên các tường lửa lọc gói tin. Hệ thống khá cơ bản này đã là thế hệ đầu tiên của cái mà sau này sẽ trở thành một tính năng kỹ thuật an toàn mạng được phát triển cao. Từ năm 1980 đến năm 1990, hai nhà nghiên cứu tại phòng thí nghiệm AT&T Bell, Dave Presetto và Howard Trickey, đã phát triển thế hệ tường lửa thứ hai, được biết đến với tên các tường lửa tầng mạch (*circuit level firewall*). Các bài báo của Gene Spafford ở Đại học Purdue, Bill Cheswick ở phòng thí nghiệm AT&T và Marcus Ranum đã mô tả thế hệ tường lửa thứ ba, với tên gọi tường lửa tầng ứng dụng (*application layer firewall*), hay tường lửa dựa proxy (*proxy-based firewall*). Nghiên cứu công nghệ của Marcus Ranum đã khởi đầu cho việc tạo ra sản phẩm thương mại đầu tiên. Sản phẩm này đã được Digital Equipment Corporation's (DEC) phát hành với tên SEAL. Đợt bán hàng lớn đầu tiên của DEC là vào ngày 13 tháng 9 năm 1991 cho một công ty hóa chất tại bờ biển phía Đông của Mỹ.

### **Lý do sử dụng Firewall**

Mạng internet ngày càng phát triển và phổ biến rộng khắp mọi nơi, lợi ích của nó rất lớn. Tuy nhiên cũng có rất nhiều ngoại tác không mong muốn đối với các cá nhân là cha mẹ hay tổ chức, doanh nghiệp, cơ quan nhà nước... như các trang web không phù hợp lứa tuổi, nhiệm vụ, lợi ích, đạo đức, pháp luật hoặc trao đổi thông tin bất lợi cho cá nhân, doanh nghiệp....Do vậy họ (các cá nhân, tổ chức, cơ quan và nhà nước) sử dụng tường lửa để ngăn chặn.

Tường lửa đóng vai trò rất quan trọng để ngăn chặn các thành phần nguy hiểm  như hacker , sâu, hay các loại virus trước khi chúng có thể xâm nhập vào máy tính.

### **Các loại Fireware**

* Có 3 loại firewall cơ bản:
* Truyền thông được thực hiện giữa một nút đơn và mạng, hay giữa một số mạng.
* Truyền thông được chặn tại tầng mạng, hay tại tầng ứng dụng.
* Tường lửa có theo dõi trạng thái của truyền thông hay không.
* Phân loại theo phạm vi của các truyền thông được lọc, có các loại sau:
* Tường lửa cá nhân hay tường lửa máy tính, một ứng dụng phần mềm với chức năng thông thường là lọc dữ liệu ra vào một máy tính đơn.
* Tường lửa mạng, thường chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các khu phi quân sự (mạng con trung gian nằm giữa mạng nội bộ và mạng bên ngoài). Một tường lửa thuộc loại này lọc tất cả truyền thông dữ liệu vào hoặc ra các mạng được kết nối qua nó.
* Phân loại theo các tầng giao thức nơi giao thông dữ liệu có thể bị chặn, có ba loại tường lửa chính:
* Tường lửa tầng mạng. Ví dụ: iptables.
* Tường lửa tầng ứng dụng. Ví dụ: TCP Wrappers.
* Tường lửa ứng dụng. Ví dụ: Hạn chế các dịch vụ FTP (File Transfer Protocol) bằng việc định cấu hình tại tệp /etc/ftpaccess.
* Phân loại có theo dõi trạng thái của truyền thông hay không:
* Tường lửa có trạng thái (*Stateful firewall*).
* Tường lửa phi trạng thái (*Stateless firewall*).

### **Nhiệm vụ.**

Nhiệm vụ cơ bản của tường lửa là bảo mật thông tin và kiểm soát trao đổi dữ liệu giữa hai vùng tin cậy khác nhau. Các vùng tin cậy (*zone of trust*) điển hình bao gồm: mạng Internet (vùng không đáng tin cậy) và mạng nội bộ (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc quyền tối thiểu (*principle of least privilege*).

### **Chức năng chính của Firewall**

* Quản lý và kiểm soát luồng dữ liệu trên mạng.
* Xác thực quyền truy cập.
* Hoạt động như một thiết bị trung gian.
* Bảo vệ tài nguyên.
* Ghi nhận và báo cáo sự kiện.

### **Firewall bảo vệ và chống lại cái gì?**

* Firewall bảo vệ:
* Dữ liệu: những thông tin cần bảo vệ do yêu cầu về:
* Bảo mật.
* Tính toàn vẹn.
* Tính kịp thời.
* Tài nguyên hệ thống.
* Danh tiếng của công ty sở hữu thông tin cần bảo về.
* Firewall chống lại những tấn công từ bên ngoài:
* Tấn công trực tiếp:
* Cách thứ nhất là dùng phương pháp dò mật khẩu trực tiếp. Thông qua các chương trình dò tìm mật khẩu với một số thông tin về người sử dụng như ngày sinh, tuổi, địa chỉ v.v…và kết hợp với thư viện do người dùng tạo ra, kẻ tấn công có thể dò được mật khẩu của bạn. Trong một số trường hợp khả năng thành công có thể lên tới 30%.
* Cách thứ hai là sử dụng lỗi của các chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được để chiếm quyền truy cập (có được quyền của người quản trị hệ thống).
* Nghe trộm: Có thể biết được tên, mật khẩu, các thông tin truyền qua mạng thông qua các chương trình cho phép đưa card giao tiếp mạng (NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền qua mạng.
* Giả mạo địa chỉ IP.
* Vô hiệu hoá các chức năng của hệ thống (deny service). Đây là kiểu tấn công nhằm làm tê liệt toàn bộ hệ thống không cho nó thực hiện các chức năng mà nó được thiết kế. Kiểu tấn công này không thể ngăn chặn được do những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.
* Lỗi người quản trị hệ thống.
* Yếu tố con người với những tính cách chủ quan và không hiểu rõ tầm quan trọng của việc bảo mật hệ thống nên dễ dàng để lộ các thông tin quan trọng cho hacker.

### **Các thành phần cơ bản của Firewall và cơ chế hoạt động**

Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

* Bộ lọc packet (Packet Filtering Router).
* Cổng ứng dụng (Application-level Gateway hay Proxy Server ).
* Cổng mạch (Circuit-level Gateway).

#### **Bộ lọc packet**

* Nguyên lý hoạt động:
* Firewall hoạt động chặt chẽ với giao thức TCP/IP. Vì giao thức này chia nhỏ các dự liệu nhận được từ các ứng dụng mạng thành các gói dữ liệu (data packet) rồi gán cho các packet này những địa chỉ để có thể nhận dạng.
* Bộ lọc packet cho phép hay từ chối mỗi packet mà nhận được. Nó kiểm tra toàn bộ dữ đoạn dữ liệu để quyết định xem dữ liệu có an toàn không.
* Ưu điểm:
* Đa số các hệ thống firewall đều được sử dụng bộ lọc gói tin. Một trong những ưu điểm của phương pháp dùng bộ lọc gói là chi phí thấp vì cơ chế lọc gói đã có sẵn trong các router.
* Ngoài ra, bộ lọc gói là trong suốt đối với người sử dụng và các ứng dụng vì vậy nó không yêu cầu người sử dụng phải thao tác gì cả.
* Nhược điểm:
* Việc định nghĩa các chế độ lọc gói là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ internet, các dạng packet header. Khi yêu cầu về lọc gói tin càng lớn, các rules càng trở nên phức tạp do đó rất khó quản lý và điều khiển.
* Do làm việc dựa trên header của các packet nên bộ lọc không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

#### **Cổng ứng dụng**

* Nguyên lý hoạt động:
* Đây là một loại firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là proxy service. Proxy service là các bộ code đặc biệt cài đặt trên cổng ra (gateway) cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy service cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị cho là chấp nhận được trong khi từ chối những đặc điểm khác.
* Ưu điểm:
* Cho phép người quản trị hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy cập bởi các dịch vụ.
* Cho phép ng­ời quản trị mạng hoàn toàn điều khiển đ­ược những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tư­ơng ứng có nghĩa là các dịch vụ ấy bị khoá.
* Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt và nó có nhật ký ghi chép lại thông tin về truy cập hệ thống.
* Luật lệ (Rules) lọc cho cổng ứng dụng dễ dàng cấu hình và kiểm tra hơn so với bộ lọc gói.
* Nhược điểm: Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client để truy cập vào các dịch vụ proxy.

#### **Cổng mạch**

* Nguyên lý hoạt động: Là một chức năng đặc biệt có thể thực hiện bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ là chuyển tiếp các kết nối TCP mà không thực hiện bất kì một hành động xử lý hay lọc gói nào.
* Ưu điểm: không cần thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Mặc dù vậy nó vẫn có thể che giấu được thông tin.

### **Thuận lợi và hạn chế của Firewall**

* Thuận lợi:
* Firewall định nghĩa một “check point” đơn giản, làm cho người sử dụng bất hợp pháp không tiếp cận được mạng được bảo vệ, giúp bảo vệ mạng chống lại các tấn công kiểu spoofing IP và routing IP.
* Firewal cung cấp một vị trí để giám sát các sự kiện liên quan đến bảo mật. Việc kiểm toán (audit) và cảnh báo (alarm) cũng có thể được cài đặt trên hệ thống firewall.
* Firewall là một hệ nền tiện lợi cho nhiều chức năng Internet không liên quan đến bảo mật, bao gồm, chức năng NAT (network address translator): ánh xạ địa chỉ mạng cục bộ thành địa chỉ Internet và chức năng quản trị mạng: kiểm toán và ghi lại các thông tin liên quan đến việc sử dụng Internet.
* Firewall có thể phục vụ như là một hệ nền cho IPSec. Khi chế độ đường hầm được triển khai, firewall có thể được sử dụng để cài đặt các mạng riêng ảo.
* Hạn chế:
* Sử dụng tường lửa cần phải xử lý một lượng lớn thông tin nên việc xử lý lọc thông tin có thể làm chậm quá trình kết nối của người kết nối.
* Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.
* Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đường dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.
* Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.
* Một ví dụ là các virus máy tính. Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của firewall.

### **Kết luận**

* Firewall cung cấp giải pháp bảo mật để ngăn ngừa các hiểm họa trực tuyến như remote login, trojan, backdoor, session hijacking, DoS & DDoS attack, virus… Hiệu quả của giải pháp bảo mật phụ thuộc vào cách cấu hình firewall và tạo các bộ lọc. Việc này đòi hỏi hiểu biết đáng kể về các giao thức mạng và về an ninh máy tính. Những lỗi nhỏ có thể biến tường lửa thành một công cụ an ninh vô dụng.
* Tùy theo quy mô và mức độ bảo mật để chọn được các loại Firewall phù hợp. Phần cứng firewall cung cấp cấp độ bảo mật ở mức độ cao, và phù hợp cho server yêu cầu mức độ bảo mật ở mức cao nhất. Phần mềm firewall thì rẻ hơn và phù hợp với người dùng cá nhân hơn.
* Tuy nhiên, với các hiểm họa lớn như DoS & DDoS…, nó có khả năng vượt qua firewall và phá hoại server. Tóm lại, firewall không đảm bảo 100% an toàn cho máy tính, hệ thống… nhưng giúp hạn chế tối đa các hiểm họa từ tấn công mạng.

## Các thuật toán mã hóa

### **Phương thức mã hóa RSA**

#### **Giới thiệu**

### Là phương thức mã hóa công khai. Do Ron Rivest, Adi Shamir và Len Adleman tại học viên MIT đề xuất năm 1977. Và hiện nay đang được sử dụng rộng rãi.

#### **Nguyên lý hoạt động**

* Mô tả sơ lược:
* Thuật toán RSA có hai [khóa](http://vi.wikipedia.org/wiki/Kh%C3%B3a_%28m%E1%BA%ADt_m%C3%A3%29): [**khóa công khai**](http://vi.wikipedia.org/wiki/Kh%C3%B3a_c%C3%B4ng_khai) (hay khóa công cộng) và [**khóa bí mật**](http://vi.wikipedia.org/w/index.php?title=Kh%C3%B3a_b%C3%AD_m%E1%BA%ADt&action=edit&redlink=1) (hay khóa cá nhân). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để [mã hóa](http://vi.wikipedia.org/wiki/M%C3%A3_h%C3%B3a). Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được.
* Để tăng tính bảo mật, n thường được chọn khá lớn. Kích thước n thường là 1024 bit hay 309 số trong hệ thập phân.
* Kích thước của các khối phải nhỏ hơn hoặc bằng log2(2).
* Với một khối M của bản rõ, khối C của bản mã (tương ứng với khối M) được tính như sau:



* Và để giải mã khối C, ta dùng công thức:



* Khóa công khai (public key) KU={e, n}.
* Khóa bí mật (private key) KR={d, n}
* Chuyển đối văn bản rõ
* Trước khi thực hiện mã hóa, ta phải thực hiện việc chuyển đổi văn bản rõ (chuyển từ M sang m) sao cho không có giá trị mà của M tạo ra văn bản không an toàn.
* Một số tiêu chuẩn, chẳng hạn như PKCS đã được thiết kế để chuyển đổi bản rõ trước khi mã hóa bằng RSA. Các phương pháp này bổ sung thêm bit vào M.
* Tạo chữ ký cho văn bản
* Thuật toán RSA còn được dùng để tạo chữ ký số cho văn bản. Giả sử Alice muốn gửi cho Bob một văn bản có chữ ký của mình. Để làm việc này, Alice tạo ra một giá trị băm (hash value) của văn bản cần ký và tính giá trị mũ d mod n của nó (giống như khi Alice thực hiện giải mã). Giá trị cuối cùng chính là chữ ký điện tử của văn bản đang xét. Khi Bob nhận được văn bản cùng với chữ ký điện tử, anh ta tính giá trị mũ e mod n của chữ ký đồng thời với việc tính giá trị băm của văn bản. Nếu 2 giá trị này như nhau thì Bob biết rằng người tạo ra chữ ký biết khóa bí mật của Alice và văn bản đã không bị thay đổi sau khi ký.
* Cần chú ý rằng các phương pháp chuyển đổi bản rõ (như RSA-PSS) giữ vai trò quan trọng đối với quá trình mã hóa cũng như chữ ký điện tử và không được dùng khóa chung cho đồng thời cho cả hai mục đích trên.

#### **An ninh**

* Độ an toàn của hệ thống RSA dựa trên 2 vấn đề của toán học: bài toán [phân tích ra thừa số nguyên tố các số nguyên lớn](http://vi.wikipedia.org/w/index.php?title=Ph%C3%A2n_t%C3%ADch_ra_th%E1%BB%ABa_s%E1%BB%91_nguy%C3%AAn_t%E1%BB%91_c%C3%A1c_s%E1%BB%91_nguy%C3%AAn_l%E1%BB%9Bn&action=edit&redlink=1) và [bài toán RSA](http://vi.wikipedia.org/w/index.php?title=B%C3%A0i_to%C3%A1n_RSA&action=edit&redlink=1). Nếu 2 bài toán trên là khó (không tìm được thuật toán hiệu quả để giải chúng) thì không thể thực hiện được việc phá mã toàn bộ đối với RSA. Phá mã một phần phải được ngăn chặn bằng các phương pháp chuyển đổi bản rõ an toàn.
* Bài toán RSA là bài toán tính căn bậc e modun n (với n là hợp số). Hiện nay phương pháp triển vọng nhất giải bài toán này là phân tích n ra thừa số nguyên tố.
* Tại thời điểm năm 2005, số lớn nhất có thể được phân tích ra thừa số nguyên tố có độ dài 663 bit với phương pháp phân tán trong khi khóa của RSA có độ dài 1024 tới 2048 bit. RSA được đảm bảo an toàn với n chọn đủ lớn. Vì vậy hiện nay thuật toán đang được dùng với n tối thiểu 2048 bit.

### **Phương thức mã hóa DES**

#### **Giới thệu**

* DES (Data Encryption Standard hay tiêu chuẩn mã hóa dữ liệu).
* Là một phương pháp mã hóa được FIPS (tiêu chuẩn xử lý thông tin Hoa Kỳ) chọn làm chuẩn năm 1976. Sau đó được sử dụng rộng rãi trên toàn thế giới.
* Do độ dài khóa qua ngắn (56 bit) nên hiện nay DES được xem là không đủ an toàn. Khóa DES đã từng bị phá trong vòng chưa đầy 24h.

#### **Nguyên lý hoạt động**

* Mô tả sơ lược.
* DES là thuật toán mã hóa khối: nó xử lý từng khối thông tin của bản rõ có độ dài xác định và biến đổi theo những quá trình phức tạp để trở thành khối thông tin của bản mã có độ dài không thay đổi. Trong trường hợp của DES, độ dài mỗi khối là 64 bit. DES cũng sử dụng khóa để cá biệt hóa quá trình chuyển đổi. Nhờ vậy, chỉ khi biết khóa mới có thể giải mã được văn bản mã. Khóa dùng trong DES có độ dài toàn bộ là 64 bit. Tuy nhiên chỉ có 56 bit thực sự được sử dụng; 8 bit còn lại chỉ dùng cho việc kiểm tra. Vì thế, độ dài thực tế của khóa chỉ là 56 bit.
* Giống như các thuật toán mã hóa khối khác, khi áp dụng cho các văn bản dài hơn 64 bit, DES phải được dùng theo một phương pháp nào đó.
* Quá trình tạo khóa con
* Đầu tiên, từ 64 bit ban đầu của khóa, 56 bit được chọn (Permuted Choice 1, hay PC-1), 8 bit còn lại bị loại bỏ. 56 bit thu được được chia làm hai phần bằng nhau, mỗi phần được xử lý độc lập. Sau mỗi chu trình, mỗi phần được dịch đi 1 hoặc 2 bit (tùy thuộc từng chu trình, nêu đó là chu trình 1,2,9,16 thì đó là dịch 1bit, còn lại thì sẽ được dich 2bit). Các khóa con 48 bit được tạo thành bởi thuật toán lựa chọn 2 (Permuted Choice 2, hay PC-2) gồm 24 bit từ mỗi phần.
* Quá trình tạo khóa con khi thực hiện giải mã cũng diễn ra tương tự nhưng các khóa con được tạo theo thứ tự ngược lại. Ngoài ra sau mỗi chu trình, khóa sẽ được dịch phải thay vì dịch trái như khi mã hóa

#### **An toàn và sự giải mã**

Mặc dù đã có nhiều nghiên cứu về phá mã DES hơn bất kỳ phương pháp mã hóa khối nào khác nhưng phương pháp phá mã thực tế nhất hiện nay vẫn là tấn công Brute-force. Nhiều đặc tính mật mã hóa của DES đã được xác định và từ đó ba phương pháp phá mã khác được xác định với mức độ phức tạp nhỏ hơn tấn công bạo lực. Tuy nhiên các phương pháp này đòi hỏi một số lượng bản rõ quá lớn (để tấn công lựa chọn bản rõ) nên hầu như không thể thực hiện được trong thực tế.

* Tấn công Brute-force (Vét cạn): là phương thức tấn công bằng cách kiểm tra tất cả các khóa có thể để tìm ra hóa thực. Tuy rằng thời gian thực hiện sẽ rất lâu tùy thuộc vào độ dài khóa nhưng với mã hóa DES thì độ dài khóa khá ngắn nên phương pháp này ban đầu được ưu tiên để phá mã DES.
* Phá mã vi sai được Eli Biham và Adi Shamir tìm ra vào cuối những năm 1980 mặc dù nó đã được IBM và NSA biết đến trước đó. Để phá mã DES với đủ 16 chu trình, phá mã vi sai cần đến 247 văn bản rõ. DES đã được thiết kế để chống lại tấn công dạng này.
* Phá mã Davies: trong khi phá mã vi sai và phá mã tuyến tính là các kỹ thuật phá mã tổng quát, có thể áp dụng cho các thuật toán khác nhau, phá mã Davies là một kỹ thuật dành riêng cho DES. Dạng tấn công này được đề xuất lần đầu bởi Davies vào cuối những năm 1980 và cải tiến bởi Biham và Biryukov (1997). Dạng tấn công mạnh nhất đòi hỏi 250 văn bản rõ, độ phức tạp là 250 và có tỷ lệ thành công là 51%.

#### **Kết luận**

Đã từng là tiêu chuẩn mã hóa trong một thời gian dài thế nhưng vì quá dễ dàng bị phá mã nên thuật toán mã hóa DES dần đi vào dĩ vãng và thay thế vào đó là thuật toán AES chúng ta sẽ tìm hiểu ngày sau đây.

### **Thuật toán mã hóa AES**

#### **Giới thệu**

* AES (Advanced Encryption Standard, hay Tiêu chuẩn mã hóa tiên tiến).
* Giống như tiêu chuẩn tiền nhiệm DES, AES được kì vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kĩ lưỡng.
* Khác với DES sử dụng mạng Feistel, Rijndael sử dụng mạng thay thế-hoán vị. AES có thể dễ dàng thực hiện với tốc độ cao bằng phần mềm hoặc phần cứng và không đòi hỏi nhiều bộ nhớ. Do AES là một tiêu chuẩn mã hóa mới, nó đang được triển khai sử dụng đại trà.

#### **Nguyên lý hoạt động**

* Mô tả sơ lược.
* Mặc dù 2 tên AES và Rijndael vẫn thường được gọi thay thế cho nhau nhưng trên thực tế thì 2 thuật toán không hoàn toàn giống nhau. AES chỉ làm việc với các khối dữ liệu (đầu vào và đầu ra) 128 bít và khóa có độ dài 128, 192 hoặc 256 bít trong khi Rijndael có thể làm việc với dữ liệu và khóa có độ dài bất kỳ là bội số của 32 bít nằm trong khoảng từ 128 tới 256 bít. Các khóa con sử dụng trong các chu trình được tạo ra bởi quá trình tạo khóa con Rijndael. Mỗi khóa con cũng là một cột gồm 4 byte. Hầu hết các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu 128 bit đầu vào được chia thành 16 byte (mỗi byte 8 bit), có thể xếp thành 4 cột, mỗi cột 4 phần tử hay là một ma trận 4x4 của các byte, nó được gọi là ma trận trạng thái, hay vắn tắt là trạng thái (tiếng Anh: state, trang thái trong Rijndael có thể có thêm cột). Trong quá trình thực hiện thuật toán các toán tử tác động để biến đổi ma trận trạng thái này.
* Quá trình mã hóa.
* Khởi động vòng lặp:
* AddRoundKey — Mỗi cột của trạng thái đầu tiên lần lượt được kết hợp với một khóa con theo thứ tự từ đầu dãy khóa.
* Vòng lặp:
* SubBytes — đây là phép thế (phi tuyến) trong đó mỗi byte trong trạng thái sẽ được thế bằng một byte khác theo bảng tra (Rijndael S-box).
* ShiftRows — dịch chuyển, các hàng trong trạng thái được dịch vòng theo số bước khác nhau.
* MixColumns — quá trình trộn làm việc theo các cột trong khối theo một phép biến đổi tuyến tính.
* AddRoundKey.
* Vòng lặp cuối:
* SubBytes.
* ShiftRows.
* AddRoundKey.

#### **An toàn và sự giải mã**

* Vào năm 2006, dạng tấn công duy nhất thành công là tấn công kênh bên. Thiết kế và độ dài của thuật toán AES (128, 192, 256 bit) là đủ an toàn để bảo mật thông tin xếp vào hàng tối mật.
* Phương pháp thường dùng nhất để tấn công các dạng mã hóa khối là thử các kiểu tấn công lên phiên bản có số chu trình thu gọn. Đối với khóa 128 bít, 192 bít và 256 bít, AES có tương ứng 10, 12 và 14 chu trình. Tại thời điểm năm 2006, những tấn công thành công được biết đến là 7 chu trình đối với khóa 128 bít, 8 chu trình với khóa 192 bít và 9 chu trình với khóa 256 bít.
* Tấn công kênh bên (Side Channel Attacks):
* Tấn công kênh bên không tấn công trực tiếp vào thuật toán mã hóa mà thay vào đó, tấn công lên các hệ thống thực hiện thuật toán có sơ hở làm lộ dữ liệu.
* Một máy chủ được thiết kế để đưa ra tối đa thông tin về thời gian có thể thu được và cuộc tấn công cần tới 200 triệu bản rõ lựa chọn. Một số người cho rằng tấn công không thể thực hiện được trên Internet với khoảng cách vài điểm mạng.

#### **Kết luận**

Hiện nay vẫn có nhiêu ứng dụng sử dụng thuật toán AES để mã hóa dữ liệu. Tuy nhiên, hệ thống mạng ngày càng phát triển và ngày càng có nhiều thuật toán mã hóa mới xuất hiện tốt hơn AES. AES vẫn đánh dấu một bước ngoặt quan trọng của công nghệ mã hóa dữ liệu.

## VNP (virtual private network)

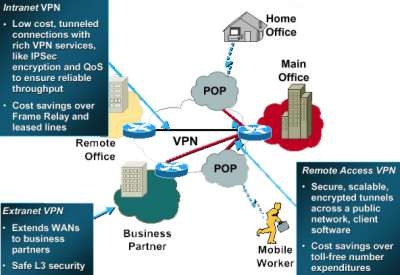
### **Đặt vấn đề**

* Nguy cơ mất an toàn thông tin trên mạng Internet:
* Nghe lén
* Giả danh
* Giả mạo
* Giải pháp:
* Point to Point link: lease line
* Mã hóa bảo mật
* Xác thực

→ Vì những lý do trên đã hình thành nên VNP (mạng riêng ảo).

### **VPN giới thiệu**

* Lợi ích của VNP
* Kết nối mạng công cộng (Internet) được đảm bảo an toàn an ninh, với những chính sách như trong mạng riêng ảo:
* Virtual
* Private
* Network
* Mở rộng mạng Intranet trên Internet.
* Bảo mật.
* Linh hoạt, không phụ thuộc vào công nghệ hạ tâng kết nối.
* Sử dụng các dịch vụ tính toán khắp nơi.
* Tăng khả năng mở rộng: kêt nối, băng thông.
* Chi phí triển khai thấp.
* Phân loại:
* Remote-Access: Hay cũng được gọi là Virtual Private Dial-up Network (VPDN), đây là dạng kết nối User-to-Lan áp dụng cho các công ty mà các nhân viên có nhu cầu kết nối tới mạng riêng (private network) từ các địa điểm từ xa. Điển hình, mỗi công ty có thể hy vọng rằng cài đặt một mạng kiểu Remote-Access diện rộng theo các tài nguyên từ một nhà cung cấp dịch vụ ESP (Enterprise Service Provider). ESP cài đặt một một công nghệ Network Access Server (NAS) và cung cấp cho các user ở xa với phần mềm client trên mỗi máy của họ. Các nhân viên từ xa này sau đó có thể quay một số từ 1-800 để kết nối được theo chuẩn NAS và sử dụng các phần mềm VPN client để truy cập mạng công ty của họ. Các công ty khi sử dụng loại kết nối này là những hãng lớn với hàng trăm nhân viên thương mại. Remote-access VPNs đảm bảo các kết nối được bảo mật, mã hoá giữa mạng riêng rẽ của công ty với các nhân viên từ xa qua một nhà cung cấp dịch vụ thứ ba (third-party).
* Site-to-Site: Bằng việc sử dụng một thiết bị chuyên dụng và cơ chế bảo mật diện rộng, mỗi công ty có thể tạo kết nối với rất nhiều các site qua một mạng công cộng như Internet. Các mạng Site-to-site VPN có thể thuộc một trong hai dạng sau:
* Intranet-based: Áp dụng trong truờng hợp công ty có một hoặc nhiều địa điểm ở xa, mỗi địa điểm đều đã có 1 mạng cục bộ LAN. Khi đó họ có thể xây dựng một mạng riêng ảo VPN để kết nối các mạng cục bộ đó trong 1 mạng riêng thống nhất.
* Extranet-based: Khi một công ty có một mối quan hệ mật thiết với một công ty khác (ví dụ như, một đồng nghiệp, nhà hỗ trợ hay khách hàng), họ có thể xây dựng một mạng extranet VPN để kết nối kiểu mạng Lan với mạng Lan và cho phép các công ty đó có thể làm việc trong một môi trường có chia sẻ tài nguyên.



### **Tính bảo mật của VNP**

Một VNP đươc thiết kế tốt thường sử dụng vài phương pháp để duy trì kết nối và giữ an toàn khi truyền dữ liệu.

* Firewall (Đã giới thiệu tại mục 2.1).
* Mã hóa (Đã giới thiệu tại mục 2.2).
* Giao thực bảo mật IPSec (Internet Protocol Security): cung cấp các tính năng bảo mật mở rộng bao gồm các thuật toán mã hóa và xác thực tốt hơn. IPSec có hai chế độ mã hoá: kênh tunnel và lớp truyền tải transport. Mã hoá kênh Tunnel mã hoá cả header và nội dung mỗi gói tin trong khi mã hoá lớp truyền tải chỉ mã hoá nội dung gói tin. Chỉ có những hệ thống sử dụng IPSec tương thích mới có khả năng tiên tiến này. Mặc dù vậy, tất cả các thiết bị phải sử dụng một khoá dùng chung và các tường lửa ở mỗi mạng phải có chính sách cấu hình bảo mật tương đương nhau. IPSec có thể mã hoá dữ liệu truyền giữa rất nhiều thiết bị, chẳng hạn như:
* Từ router đến router
* Từ firewall đến router
* Từ PC đến router
* Từ PC đến server
* Máy chủ xác thực, xác nhận và quản lý tài khoản AAA Server (Authentication, Authorization, Accounting Server) được sử dụng để tăng tính bảo mật trong truy nhập từ xa của VPN. Khi một yêu cầu được gửi đến để tạo nên một phiên làm việc, yêu cầu này phải đi qua một AAA server đóng vai trò proxy. AAA sẽ kiểm tra:
* Bạn là ai (xác thực)
* Bạn được phép làm gì (xác nhận)
* Bạn đang làm gì (quản lý tài khoản)

Các thông tin về tài khoản sử dụng đặc biệt hữu ích khi theo dõi người dùng nhằm mục đích bảo mật, tính hoá đơn hoặc lập báo cáo.

### **Các kĩ thuật sử dụng trong VNP**

Phụ thuộc vào kiểu VPN (truy nhập từ xa Remote-Access hay kết nối ngang hàng Site-to-Site), bạn sẽ cần một số thành phần nhất định để hình thành VPN, bao gồm:

* Phần mềm máy trạm cho mỗi người dùng xa.
* Các thiết bị phần cứng riêng biệt, ví dụ như: bộ tập trung (VPN Concentrator) hoặc tường lửa (Secure PIX Firewall).
* Các máy chủ VPN sử dụng cho dịch vụ quay số.
* Máy chủ truy cập NAS (Network Access Server) dùng cho các người dùng VPN ở xa truy nhập.
* Trung tâm quản lý mạng và chính sách VPN

Hiên nay do chưa có tiêu chuẩn rộng rãi để triển khai VPN, rất nhiều công ty đã tự phát triển các giải pháp trọn gói cho riêng mình. Ví dụ, Cisco đã đưa ra một vài giải pháp cho VPN bao gồm:

* Bộ tập trung VPN (VPN Concentrator): Tích hợp các ưu điểm tiên tiến nhất của mã hoá và xác nhận, bộ tập trung Cisco được chế tạo riêng biêt cho tính năng truy cập VPN từ xa. Chúng cung cấp khả năng sử dụng, hiệu năng cao, dễ nâng cấp mở rộng và bao gồm nhiều thành phần gọi là bộ xử lýã hoá có khả năng mở rộng (Scalabe Encryption Pcessing - SEP), cho phép người dùng dễ dàng tăng thêm dung lượng và khả năng xử lý. Các bộ tập trung rất phù hợp cho các doanh nghiệp với khoảng 100 số người truy cập VPN từ xa hoặc ít hơn truy nhập đến mạng của tổ chức có khoảng 10,000 người sử dụng đồng thời.
* Bộ đinh tuyến VPN thông minh (Cisco's VPN-optimized routers) cung cấp khả năng định tuyến, bảo mật và chất lượng dịch vụ mở rộng. Dựa trên nền tảng phần mềm hệ điều hành mạng internat của Cisco IOS (Internet Operating System), đây là một bộ định tuyến rất phù hợp cho hầu hết các trường hợp, từ văn phòng nhỏ/văn phòng gia đình SOHO (small-office/home-office) truy nhập đến trung tâm VPN, hoặc đến các doanh nghiệp quy mô lớn.
* Tường lửa bảo mật - Cisco Secure PIX Firewall: Bộ PIX (Private Internet eXchange) Firewall tích hợp bộ phiên dịch địa chỉ mạng động, máy chủ proxy, bộ lọc gói tin, tường lửa và VPN trong một phần cứng duy nhất. Thay thế cho việc sử dụng Cisco IOS, thiết bị này có dung lượng thông tin cao hơn phù hợp cho khả năng quản lý nhiều giao thức và rất tinh vi đặc biêt là IP.

### **Kết luận**

VPN là một giải pháp tốt cho công ty để kết nối nhân viên và các bạn hàng mà không phụ thuộc vào việc họ đang ở đâu.

# Một số phương pháp tấn công và cách phòng tránh

## Sniff (Nghe lén)

### **Khái niệm**

Sniffer là một chương trình nghe trộm gói tin (*packet sniffer*) (còn gọi là chương trình phân tích mạng, chương trình phân tích giao thức hay chương trình nghe trộm Ethernet) là một phần mềm có khả năng chặn và ghi lại giao thông dữ liệu qua một mạng viễn thông số hoặc một phần của một mạng dựa trên những đặc điểm của giao thức TCP/IP.

Sniffer ban đầu được sử dụng để các nhà quản trị mạng theo dõi và bảo trì hệ thống mạng của mình. Tuy nhiên sau này các hacker lại sử dụng nó như một công cụ với mục đích đánh hơi, nghe lén các thông tin trang mạng.

### **Sơ lược về cách tấn công**

Khi các dòng dữ liệu di chuyển qua lại một mạng, chương trình nghe trộm bắt lấy từng gói tin rồi giải mã và phân tích nội dung của nó theo RFC hoặc các đặc tả thích hợp khác. Tùy theo cấu trúc mạng người ta có thể nghe trộm tất cả hoặc chỉ một phần của giao thông dữ liệu từ một máy trong mạng. Đối với các mục đích theo dõi mạng (*network monitoring*), người ta có thể theo dõi tất cả các gói tin trong một mạng LAN bằng cách sử dụng một thiết bị chuyển mạch với một cái gọi là cổng theo dõi (nó lặp lại tất cả các gói tin đi qua tất cả các cổng của thiết bị chuyển mạch).

Những điều kiện để Sniff xảy ra:

* Sniff có thể hoạt động trong mạng LAN, mạng WAN, mạng WLAN.
* Điều kiện cần chỉ là dùng cùng Subnet Mark với Sniffer.
* Ngoài ra ta còn cần một công cụ để bắt và phân tích gói tin như: Cain&Abel, Ettercap, HTTP sniffer.

### **Các loại sniff và cơ chế hoạt động**

* Active:
* Môi trường: chủ yếu hoạt động trong môi trường có các thiết bị chuyển mạch gói. Phổ biến hiện nay là các dạng mạch sử dụng switch.
* Cơ chế hoạt động: Chủ yếu hiện nay thường dùng cơ chế ARP và RARP

(2 cơ chế chuyển đổi từ IP sang MAC và từ MAC sang IP) bằng cách phát đi các gói tin đầu độc, mà cụ thể ở đây là phát đi các gói thông báo cho máy gởi gói tin là “tôi là người nhận” mặc dù không phải là “người nhận”.

* Đặc điểm: do phải gởi gói tin đi nên có thể chiếm băng thông mạng. Nếu sniff quá nhiều máy trong mạng thì lượng gói gởi đi sẽ rất lớn (do liên tục gởi đi các gói tin giả mạo) có thể dẫn đến nghẽn mạng hay gây quá tải trên chính NIC của máy đang dùng sniff (thắt nút cổ chai).
* Hacker sử dụng các loại tấn công:
* MAC flooding:. Hacker sẽ gởi những gói ARP reply giả tạo với số lượng khổng lồ nhằm làm tràn bộ nhớ switch từ đó switch sẽ chạy chế độ forwarding mà không chuyển mạch gói.
* Giả MAC: Các sniffer sẽ thay đổi MAC của mình thành MAC của một máy hợp lệ và qua được chức năng lọc MAC của thiết bị.
* Đầu độc DHCP: Hacker giả mạo địa chỉ IP của mình là địa chỉ của gateway, từ đó mọi host trong mạng đều gửi gói tin đến gateway nhưng thực chất là đến máy của hacker.
* Passive:
* Môi trường: chủ yếu hoạt động trong môi trường không có các thiết bị chuyển mạch gói. Phổ biến hiện nay là các dạng mạng sử dụng hub, hay các mạng không dây.
* Cơ chế hoạt động: do không có các thiết bị chuyển mạch gói nên các host phải bị broadcast các gói tin đi trong mạng từ đó có thể bắt gói tin lại xem (dù host nhận gói tin không phải là nơi đến của gói tin đó).
* Đặc điểm: do các máy tự broadcast các gói nên hình thức sniff này rất khó phát hiện.

### **Cách phát hiện và phòng chống**

#### **Đối với active sniff**

1. Cách phát hiện

* Dựa vào quá trình đầu độc arp của sniffer để phát hiện.
* Vì phải đầu độc ARP nên sniffer sẽ liên tục gởi các gói tin đầu độc tới các victim. Do đó, ta có thể dùng một số công cụ bắt gói trong mạng để có thể phát hiện.
* Một cách khác ta có thể kiểm tra bảng ARP của host. Nếu ta thấy trong bảng ARP này có hai MAC giống nhau thì lúc này có khả năng mạng đang bị sniffer.
* Dựa trên băng thông:
* Do quá trình gởi gói tin đầu độc của sniffer nên quá trình này có thể chiếm băng thông, từ đây ta có thể dùng một số công cụ kiểm tra băng thông để phát hiện.
* Tuy nhiên cách này không hiệu quả và chính xác cũng không cao.
* Một số công cụ phát hiện sniff hay phát hiện đầu độc ARP:
* Xarp
* Arpwatch
* Symantec EndPoint.

1. Cách phòng chống

* Công cụ kiểm tra băng thông: Như đã nêu trên các sniffer có thể gây nghẽn mạng do đó có thể dùng các công cụ kiểm tra băng thông. Tuy nhiên, cách làm này không hiệu quả.
* Công cụ bắt gói tin: Các sniffer phải đầu độc ARP nên sẽ gởi arp đi liên tục, nếu dùng các công cụ này ta có thể thấy được ai đang sniff trong mạng. Cách này tương đối hiệu quả hơn, nhưng có một vài công cụ sniff có thể giả IP và MAC để đánh lừa.
* Thiết bị: Đối với thiết bị ta có thể dùng các loại có chức năng lọc MAC để phòng chống. Riêng với switch có thể dùng thêm chức năng VLAN trunking, có thể kết hợp thêm chức năng port security (tương đối hiệu quả do dùng VLAN và kết hợp thêm các chức năng bảo mật).
* Cách khác: Ngoài ra ta có thể cấu hình SSL, tuy hiệu quả, nhưng chưa cao vẫn có khả năng bị lấy thông tin.

#### **Đối với passive sniff**

1. Cách phát hiện

* Khó có khả năng phát hiện, vì bất kỳ host nào trong mạng cũng có thể bắt được gói tin.
* Tuy nhiên, dạng mạng để loại sniff này hoạt động chủ yếu dạng mạng thường dùng trong gia đình rất ít sử dụng cho doanh nghiệp.
* Tuy nhiên, hiện nay các doanh nghiệp thường dùng mạng không dây cho các máy tính xách tay thì có thể sử dụng thêm các tính năng lọc MAC của thiết bị, hay có thể xác thực bằng tài khoản, mật khẩu hay khóa truy cập.

1. Cách phòng chống

Thay thế các hub bằng các switch, lúc này các gói tin sẽ không còn broadcast đi nữa , nhưng lúc này ta lại đứng trước nguy cơ bị sniff dạng active.

### **Mức độ ảnh hưởng đến hệ thống**

Sniff là hình thức nghe lén thông tin trên mạng nhằm khai thác hiệu quả hơn tài nguyên mạng, theo dõi thông tin bất hợp pháp. Tuy nhiên, sau này các hacker dùng sniff để lấy các thông tin nhạy cảm như password, thông tin cá nhân... Do đó, sniff cũng là một cách hack.

Sniff thường tác động đến các gói tin, ít tác động mạnh đến phần hệ thống nên sniff rất khó phát hiện. Do đó, tuy sniff hoạt động đơn giản nhưng rất hiệu quả.

Do gần như không trực tiếp tác động lên hệ thống mạng nên các hình thức sniff sau khi hoạt động thường ít để lại dấu vết hay hậu quả nghiêm trọng.

## Phishing

### **Khái niệm**

Tấn công giả mạo (thuật ngữ tiếng Anh: phishing, biến thể từ fishing, nghĩa là câu cá, có thể ảnh hưởng từ chữ phreaking, nghĩa là sử dụng điện thoại người khác không trả phí, ám chỉ việc "nhử" người dùng tiết lộ thông tin mật) là một hành vi giả mạo ác ý nhằm lấy được các thông tin nhạy cảm như tên người dùng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành một chủ thể tin cậy trong một giao dịch điện tử .

Cách thực hiện chủ yếu là đánh lừa người dùng truy cập vào một web giả mô phỏng lại giao diện trang web đăng nhập (login page) của các website có thật. Sau đó, kẻ lừa đảo sẽ dẫn dụ nạn nhân (victim) điền các thông tin vào trang “dỏm” đó rồi truyền tải đến anh ta (thay vì đến server hợp pháp) để thực hiện hành vi đánh cắp thông tin bất hợp pháp mà người sử dụng không hay biết. Ngay cả khi có sử dụng chứng thực máy chủ, có khi vẫn phải cần vài kĩ năng phức tạp mới xác định được website là giả mạo.

### **Thời gian xuất hiện**

Một kĩ thuật tấn công giả mạo đã được mô tả chi tiết trong một bài báo khoa học và thuyết minh của “Nhóm Người dùng HP Toàn cầu” vào năm 1987. Tuy nhiên, thuật ngữ "phishing" được đề cập lần đầu tiên trên nhóm tin “Usenet” vào ngày 2 tháng 1 năm 1996, dù thuật ngữ này có thể đã xuất hiện từ trước đó trong bản in của tạp chí dành cho hacker “2600” .

### **Sơ lược cách tấn công**

Trước đây, hacker thường sử dụng trojan (gián điệp) đến máy nạn nhân nhằm ăn cắp thông tin như password. Sau này cách lừa đảo lấy thông tin như Phishing được sử dụng nhiều hơn. Phương pháp phổ biến nhất của phishing là sử dụng một số form được thiết kế để tạo một liên kết tới một địa chỉ email có vẻ như thuộc về một tổ chức đang tin cậy hoặc một tổ chức giả mạo. Đường dẫn URLs sai chính tả hoặc việc sử dụng tên miền phụ là thủ thuật phổ biến được sử dụng hiện nay bởi những hacker.

Phishing gồm 2 bước chính:

* Tìm cách lừa người dùng đăng nhập vào trang web đăng nhập giả. Cách làm chính là thông qua gửi một email có chưa URL đến trang web giả.
* Tạo một trang web giả giống với trang web thật.
* Không chỉ có vậy, hacker còn kết hợp nhiều xảo thuật khác như tạo những email (giả) cả địa chỉ lẫn nội dung sao cho có sức thu hút, mã hóa đường link (URL) trên thanh address bar, tạo IP server giả…

### **Cách phòng chống**

Phòng chống Phishing là không khó. Phishing chủ yếu đánh vào sự tin tưởng của người dùng khi thực hiện nhưng giao dịch online. Vì thế cách tốt nhất là người dùng phải cẩn thận khi nhận được yêu cầu cung cấp thông tin nhạy cảm.

Nếu nhấn vào liên kết ở email đó nó đưa bạn đến một trang đăng nhập (giả). Dù bên ngoài nó giống hệt trang thật, ngay cả địa chỉ hay thanh trạng thái nhìn cũng có vẻ thật. Nhưng nếu bạn xem kỹ liên kết trên thanh address bar thì bạn sẽ thấy ở phía sau chữ @ mới là địa chỉ thật. Bạn nên quan sát kĩ trước khi điền thông tin. Tốt hơn hết là xem mã nguồn (view source) của form thì rõ là form thông tin không phải truyền đến citibank mà là đến một nơi khác.

Với cách tiếp cận theo kiểu “biết cách tấn công để phòng thủ” trên, chúng ta sẽ thấy rõ hơn bản chất của một cuộc tấn công phishing – tấn công đơn giản, nhưng hiệu quả thì rất cao. Một khi bạn hiểu được cách thức tấn công thì chắc rằng bạn cũng sẽ có cách đối phó thích hợp.

* Tóm lại:
* Cẩn thận với những email lạ, đặc biệt là những email yêu cầu cung cấp thông tin dù vẫn biết là phải tránh nhưng không ít trường hợp đều chủ quan.
* Xem kỹ nội dung có chính xác, có giống với những biểu mẫu thường gặp không. Nếu sai chính tả như trên thì bạn nên xem xét lại.
* Nếu có yêu cầu xác nhận thì xem kỹ liên kết, nếu có ký tự là như @ hay %01 thì có khả năng giả mạo.
* Với các trang xác nhận thông tin quan trọng, họ luôn dùng giao thức http secure (có ‘s’ sau http) nên địa chỉ có dạng http**s**://.... chứ không phải là http:// thường. Ngân hàng kêu ta xác nhận lại dùng http:// “thường” thì chắc là ngân hàng… giả.
* Nên thường xuyên cập nhật các miếng vá lỗ hổng bảo mật cho trình duyệt (web browser). Cài thêm chương trình phòng chống virus, diệt worm, trojan.

### **Mức độ ảnh hưởng**

Phishing là hình thức gian lận, lừa người dùng cung cấp thông tin cá nhân đặc biệt là thông tin về tài khoản ngân hàng, giao dịch trực tuyến… Sau đó sử dụng những thông tin đó chiếm đoạt tài chính của nạn nhân.

Phishing tấn công đơn giản nhưng mang lại hiệu quả cao và còn có thể mở rộng tấn công cho nên tình trạng lừa đảo này ngày càng có dấu hiệu tăng lên về số lượng và quy mô .

Hằng năm trên thế giới xảy ra hàng loạt vụ lừa đảo, chiếm dụng tài khoản ngân hàng của người dùng, thiệt hại lên đến hàng triệu USD.

Hiện nay không chỉ có ngân hàng mà nó còn mở rộng sang nhiều lĩnh vực khác. Năm 2011 nhiều tên tuổi đình đám của thế giới như: Google, Sony, IMF cũng đã bị hacker tấn công chiếm đoạt thông tin.

## SQL Injection

### **Khái niệm**

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,… trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

### **Thời gian xuất hiện.**

Ban đầu SQL Injection được công bố lần đầu tiên như một lưu ý trong một bài viết về phương pháp khai thác lỗ hổng dịch vụ Web của Microsoft. Bài viết này được xuất hiện đầu tiên tại số thứ 54 của tạp chí Phrack (giáng sinh năm 1998), lúc đó là một tạp chí thường kỳ về chủ đề Hacking. Số báo thứ 54 đó được biết tới như là điểm khởi đầu của loại hình SQL Injection.

### **Cách thức tấn công**

Có bốn dạng tấn công thường gặp bao gồm: vượt qua kiểm tra lúc đăng nhập, sử dụng câu lệnh SELECT, sử dụng câu lệnh INSERT, sử dụng các stored-procedures.

#### **Dạng tấn công vượt qua kiểm tra lúc đăng nhập**

Với dạng tấn công này, tin tặc có thể dễ dàng vượt qua các trang đăng nhập nhờ vào lỗi khi dùng các câu lệnh SQL thao tác trên cơ sở dữ liệu của ứng dụng web. Thông thường để cho phép người dùng truy cập vào các trang web được bảo mật, hệ thống thường xây dựng trang đăng nhập để yêu cầu người dùng nhập thông tin về tên đăng nhập và mật khẩu. Sau khi người dùng nhập thông tin vào, hệ thống sẽ kiểm tra tên đăng nhập và mật khẩu có hợp lệ hay không để quyết định cho phép hay từ chối thực hiện tiếp.

Ví dụ, trong trường hợp sử dụng ASP, người ta có thể dùng 2 trang : 1 trang HTML để hiển thị Form nhập liệu và 1 trang ASP để xử lý thông tin nhập vào từ phía người dùng như sau:

- Trang nhập liệu: *login.htm*

*<form action="ExecLogin.asp" method="post">*

*Username: <input type="text" name="fUSRNAME"><br />*

*Password: <input type="password" name="fPASSWORD"><br />*

*<input type="submit">*

*</form>*

Trang xử lý nhập liệu*: execlogin.asp*

*<%*

*Dim vUsrName, vPassword, objRS, strSQL*

*vUsrName = Request.Form("fUSRNAME")*

*vPassword = Request.Form("fPASSWORD")*

*strSQL = "SELECT \* FROM T\_USERS " & \_*

*"WHERE USR\_NAME=' " & vUsrName & \_*

*" ' and USR\_PASSWORD=' " & vPassword & " ' "*

**Set** *objRS = Server.CreateObject("ADODB.Recordset")*

*objRS.Open strSQL, "DSN=..."*

**If** *(objRS.EOF) Then*

*Response.Write "Invalid login."*

**Else**

*Response.Write "You are logged in as " & objRS("USR\_NAME")*

*End* **If**

**Set** *objRS = Nothing %>*

Chỗ sơ hở trong đoạn mã xử lý nhập liệu trên nằm ở chỗ dữ liệu nhập vào từ người dùng được dùng để xây dựng trực tiếp câu lệnh SQL. Chính điều này cho phép tin tặc có thể điều khiển câu truy vấn sẽ được thực hiện. Ví dụ, nếu người dùng nhập chuỗi trong ngoặc sau vào trong cả 2 ô nhập liệu username/password của trang login.htm là: ('OR*=').* Lúc này, câu truy vấn sẽ được gọi thực hiện là:

SELECT \* FROM T\_USERS WHERE USR\_NAME =''OR''='' AND USR\_PASSWORD= ''OR''=''

Câu truy vấn này là hợp lệ và sẽ trả về tất cả các bản ghi của T\_USERS và đoạn mã tiếp theo xử lí người dùng đăng nhập bất hợp pháp này như là người dùng đăng nhập hợp lệ.

#### **Dạng tấn công sử dụng câu lệnh SELECT**

Dạng tấn công này phức tạp hơn. Để thực hiện được kiểu tấn công này, kẻ tấn công phải có khả năng hiểu và lợi dụng các sơ hở trong các thông báo lỗi từ hệ thống để dò tìm các điểm yếu khởi đầu cho việc tấn công. Ví dụ, trong các trang tìm kiếm. Các trang này cho phép người dùng nhập vào các thông tin tìm kiếm như Họ, Tên, … Đoạn mã thường gặp là:

*<%*

*Dim vAuthorName, objRS, strSQL*

*vAuthorName = Request("fAUTHOR\_NAME")*

*strSQL = "SELECT \* FROM T\_AUTHORS WHERE AUTHOR\_NAME =' " & \_ vAuthorName & " ' "*

*Set objRS = Server.CreateObject("ADODB.Recordset")*

*objRS.Open strSQL, "DSN=..."*

*…*

*Set objRS = Nothing %>*

Tương tự như trên, tin tặc có thể lợi dụng sơ hở trong câu truy vấn SQL để nhập vào trường tên tác giả bằng chuỗi giá trị:

*' UNION SELECT ALL SELECT OtherField FROM OtherTable WHERE ' '=' (\*)*

Lúc này, ngoài câu truy vấn đầu không thành công, chương trình sẽ thực hiện thêm lệnh tiếp theo sau từ khóa UNION nữa. Giả sử đoạn mã nhập vào là:

*' DROP TABLE T\_AUTHORS --*

Câu truy vấn sẽ thực hiện việc xóa bảng.

#### **Dạng tấn công sử dung câu lệnh INSERT**

Thông thường các ứng dụng web cho phép người dùng đăng kí một tài khoản để tham gia. Chức năng không thể thiếu là sau khi đăng kí thành công, người dùng có thể xem và hiệu chỉnh thông tin của mình. SQL injection có thể được dùng khi hệ thống không kiểm tra tính hợp lệ của thông tin nhập vào. Ví dụ, một câu lệnh INSERT có thể có cú pháp dạng:

*INSERT INTO TableName VALUES('Value One', 'Value Two', 'Value Three')*

Nếu đoạn mã xây dựng câu lệnh SQL có dạng :

*<%*

*strSQL = "INSERT INTO TableName VALUES(' " & strValueOne & " ', ' " \_ & strValueTwo & " ', ' " & strValueThree & " ') "*

*Set objRS = Server.CreateObject("ADODB.Recordset")*

*objRS.Open strSQL, "DSN=..."*

*…*

*Set objRS = Nothing %>*

Thì chắc chắn sẽ bị lỗi SQLi, bởi vì nếu ta nhập vào trường thứ nhất ví dụ như:

*' + (SELECT TOP 1 FieldName FROM TableName) + '*

Lúc này câu truy vấn sẽ là :

*INSERT INTO TableName VALUES(' ' + (SELECT TOP 1 FieldName FROM TableName) + ' ', 'abc', 'def')*

Khi đó, lúc thực hiện lệnh xem thông tin, xem như bạn đã yêu cầu thực hiện thêm một lệnh nữa đó là:

*SELECT TOP 1 FieldName FROM TableName*

#### **Dạng tấn công sử dụng store-procedures**

Việc tấn công bằng stored-procedures sẽ gây tác hại rất lớn nếu ứng dụng được thực thi với quyền quản trị hệ thống 'sa'. Ví dụ, nếu ta thay đoạn mã tiêm vào dạng: ' ; EXEC xp\_cmdshell ‘cmdd.exe dir C: '. Lúc này hệ thống sẽ thực hiện lệnh liệt kê thư mục trên ổ đĩa C:\ cài đặt server. Việc phá hoại kiểu nào tuỳ thuộc vào câu lệnh đằng sau cmd.exe.

### **Kỹ thuật an ninh dùng để phòng chống SQL Injection**

Biết được về mức độ ảnh hưởng của SQL Injection là rất lớn nên các nhà phát triển web và các chuyên gia bảo mật không ngừng tìm ra những cách để chống lại lỗ hổng bảo mật này, cho đến hiện nay đã có rất nhiều cách thức củng như thủ thuật để chống lại, có thể kể đến một số cách sau đây:

#### **Kiểm soát chặt chẽ dữ liệu nhập vào**

*<%*

*Function EscapeQuotes(sInput)*

*sInput = replace(sInput, " ' ", " ' ' ")*

*EscapeQuotes = sInput*

*End Function*

*%>*

Trong trường hợp dữ liệu nhập vào là số, lỗi xuất phát từ việc thay thế một giá trị được tiên đoán là dữ liệu số bằng chuỗi chứa câu lệnh SQL bất hợp pháp. Để tránh điều này, đơn giản hãy kiểm tra dữ liệu có đúng kiểu hay không bằng hàm Is Numeric().

Ngoài ra có thể xây dựng hàm loại bỏ một số kí tự và từ khóa nguy hiểm như: ;--, select, insert, xp\_, … ra khỏi chuỗi dữ liệu nhập từ phía người dùng để hạn chế các tấn công dạng này:

*<%*

*Function KillChars(sInput)*

*dim badChars*

*dim newChars*

*badChars = array("select", "drop", ";", "--", "insert", "delete", "xp\_")*

*newChars = strInput*

*for i = 0 to uBound(badChars)*

*newChars = replace(newChars, badChars(i), "")*

*next*

*KillChars = newChars*

*End Function*

*%>*

#### **Thiết lập cấu hình an toàn cho hệ quản trị cơ sở dữ liệu**

Cần có cơ chế kiểm soát chặt chẽ và giới hạn quyền xử lí dữ liệu đến tài khoản người dùng mà ứng dụng web đang sử dụng. Các ứng dụng thông thường nên tránh dùng đến các quyền như dbo hay sa.Quyền càng bị hạn chế, thiệt hại càng ít. Ngoài ra để tránh các nguy cơ từ SQL Injection attack, nên chú ý loại bỏ bất kì thông tin kĩ thuật nào chứa trong thông điệp chuyển xuống cho người dùng khi ứng dụng có lỗi. Các thông báo lỗi thông thường tiết lộ các chi tiết kĩ thuật có thể cho phép kẻ tấn công biết được điểm yếu của hệ thống

#### **Sử dụng thủ thuật.**

Ngoài các cách trên, một số web master còn sử dụng một số thủ thuật để chống lại tấn công SQL Injection đơn giản và tạm thời như: Dùng hàm để loại bỏ các câu lệnh và ký tự không cần thiết để người tấn công không thể dung các câu lệnh để tấn công.

### **Mức độ ảnh hưởng**

Cho đến nay, có thể nói rằng SQL Injection như là một trong những lỗ hổng có mức tàn phá ghê gớm nhất tới hoạt động kinh doanh của các doanh nghiệp, tổ chức, làm thất thoát các thông tin mang tính nhạy cảm được lưu trong cơ sở dữ liệu của ứng dụng như là Tên người dùng, mật khẩu, địa chỉ, địa chỉ thư điện tử, số điện thoại, thông tin thẻ tín dụng…

## Tấn công từ chối dịch vị (DDoS)

### **Khái niệm**

Tấn công từ chối dịch vụ là tên gọi chung của cách tấn công làm cho một hệ thống nào đó bị quá tải không thể cung cấp dịch vụ, làm gián đoạn hoạt động của hệ thống hoặc hệ thống phải ngưng hoạt động**.**

### **Thời gian xuất hiện**

Vào năm 1998 Chương trình Trinoo Distributed Denial of Service (DDoS) được viết bởi Phifli đươc coi như mở đầu cho hình thức tấn công từ chối dịch vụ.

### **Các cách tấn công**

#### **SYN Attack**

Được xem là một trong những kiểu tấn công DoS kinh điển nhất. Lợi dụng sơ hở của thủ tục TCP khi “bắt tay ba bước”, mỗi khi client muốn thực hiện kết nối với server thì nó thực hiện việc bắt tay ba bước thông qua các gói tin (packet):

* Bước 1: client sẽ gửi gói tin (packet chứa SYN=1) đến máy chủ để yêu cầu kết nối.
* Bước 2: khi nhận được gói tin này, server gửi lại gói tin SYN/ACK để thông báo cho client biết là nó đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ dành một phần tài nguyên để nhận và truyền dữ liệu. Ngoài ra, các thông tin khác của client như địa chỉ IP và cổng (port) cũng được ghi nhận.
* Bước 3: cuối cùng client hoàn tất việc bắt tay ba bước bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối.

Do TCP là thủ tục tin cậy trong việc giao nhận nên trong lần bắt tay thứ hai, server gửi gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho client đến khi nhận được hồi đáp của client.

Điểm mấu chốt ở đây là làm cho client không hồi đáp cho Server, và có càng nhiều, càng nhiều client như thế trong khi server vẫn lặp lại việc gửi packet đó và giành tài nguyên để chờ trong lúc tài nguyên của hệ thống là có giới hạn.

Thường, để giả địa chỉ IP, các hacker hay dùng Raw Sockets (không phải gói tin TCP hay UDP) để giả mạo hay ghi đè giả lên IP gốc của gói tin. Khi một gói tin SYN với IP giả mạo được gửi đến server, nó cũng như bao gói tin khác, vẫn hợp lệ đối với server và server sẽ cấp vùng tài nguyên cho đường truyền này, đồng thời ghi nhận toàn bộ thông tin và gửi gói SYN/ACK ngược lại cho client.

Vì địa chỉ IP của client là giả mạo nên sẽ không có client nào nhận được SYN/ACK packet này để hồi đáp cho máy chủ. Sau một thời gian không nhận được gói tin ACK từ client, server nghĩ rằng gói tin bị thất lạc nên lại tiếp tục gửi tiếp SYN/ACK, cứ như thế, các kết nối tiếp tục mở.

#### Flood attack

Một kiểu tấn công DoS nữa cũng rất hay được dùng vì tính đơn giản của nó và vì có rất nhiều công cụ sẵn có hỗ trợ đắc lực cho kẻ tấn công là Flood Attack, chủ yếu thông qua các website.

Về nguyên tắc, các website đặt trên máy chủ khi chạy sẽ tiêu tốn một lượng tài nguyên nhất định của máy chủ. Dựa vào đặc điểm đó, những kẻ tấn công dùng các phần mềm như smurf chẳng hạn để liên tục yêu cầu máy chủ phục vụ trang web đó để chiếm dụng tài nguyên.

#### **Smurf attack**

Là thủ phạm sinh ra cực nhiều giao tiếp ICMP (ping) tới địa chỉ Broadcast của nhiều mạng với địa chỉ nguồn là mục tiêu cần tấn công. Chúng ta cần lưu ý là: Khi ping tới một địa chỉ là quá trình hai chiều – Khi máy A ping tới máy B máy B reply lại hoàn tất quá trình. Khi tôi ping tới địa chỉ Broadcast của mạng nào đó thì toàn bộ các máy tính trong mạng đó sẽ Reply lại tôi. Nhưng giờ tôi thay đổi địa chỉ nguồn, thay địa chỉ nguồn là máy C và tôi ping tới địa chỉ Broadcast của một mạng nào đó, thì toàn bộ các máy tính trong mạng đó sẽ reply lại vào máy C chứ không phải tôi và đó là tấn công Smurf. Kết quả đích tấn công sẽ phải chịu nhận một đợt Reply gói ICMP cực lớn và làm cho mạng bị dớt hoặc bị chậm lại không có khả năng đáp ứng các dịch vụ khác.

#### **Tấn công dịch vụ phân tán DDoS**

Để thực hiện thì kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính/mạng máy tính trung gian (đóng vai trò zombie) từ nhiều nơi để đồng loạt gửi ào ạt các gói tin với số lượng rất lớn nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó. Làm cho sever hoàn toàn tê liệt. Theo cách này thì dù băng thông có bao nhiêu đi chăng nữa thì cũng không thể chịu đựng được số lượng hàng triệu các gói tin đó nên hệ thống không thể hoạt động được nữa và như thế dẫn đến việc các yêu cầu hợp lệ khác không thể nào được đáp ứng, server sẽ bị “đá văng” khỏi internet.

#### **Tấn công từ chối dịch vụ phản xạ nhiều vùng DRDOS.**

Xuất hiện vào đầu năm 2002, là kiểu tấn công mới nhất, mạnh nhất trong họ DoS. Nếu được thực hiện bởi kẻ tấn công có tay nghề thì nó có thể hạ gục bất cứ hệ thống nào trên thế giới trong phút chốc. Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy chủ, tức là làm tắc nghẽn hoàn toàn đường kết nối từ máy chủ vào xương sống của Internet và tiêu hao tài nguyên máy chủ. Trong suốt quá trình máy chủ bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy chủ đó. Tất cả các dịch vụ chạy trên nền TCP/IP như DNS, HTTP, FTP, POP3,... đều bị vô hiệu hóa. Về cơ bản, DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS. Nó có kiểu tấn công SYN với một máy tính đơn, vừa có sự kết hợp giữa nhiều máy tính để chiếm dụng băng thông như kiểu DDoS. Kẻ tấn công thực hiện bằng cách giả mạo địa chỉ của server mục tiêu rồi gửi yêu cầu SYN đến các server lớn như Yahoo, Micorosoft, chẳng hạn để các server này gửi các gói tin SYN/ACK đến server mục tiêu. Các server lớn, đường truyền mạnh đó đã vô tình đóng vai trò zoombies cho kẻ tấn công như trong DDoS.

Quá trình gửi cứ lặp lại liên tục với nhiều địa chỉ IP giả từ kẻ tấn công, với nhiều server lớn tham gia nên server mục tiêu nhanh chóng bị quá tải, bandwidth bị chiếm dụng bởi server lớn. Tính “nghệ thuật” là ở chỗ chỉ cần với một máy tính với modem 56kbps, một hacker lành nghề có thể đánh bại bất cứ máy chủ nào trong giây lát mà không cần chiếm đoạt bất cứ máy nào để làm phương tiện thực hiện tấn công.

### **Cách thức phòng chống:**

* + Tăng cường khả năng xử lý của hệ thống:
* Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web.
* Nâng cấp hệ thống máy chủ.
* Nâng cấp đường truyền và các thiết bị liên quan.
* Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển,v.v…
  + Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối nhằm tấn công hệ thống.
  + Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.
  + Ngoài ra ta củng có thể cụng một số công cụ để chống lại như:
* Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ.
* Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,…

### **Mức độ ảnh hưởng:**

Một cuộc tấn công mạng theo phương thức tấn công từ chối dịch vụ (DDoS) phổ biến hiện nay có thể làm tê liệt những hệ thống mạng doanh nghiệp, hay một ngân hàng gây thiệt hại hàng tỉ đồng và không chỉ thiệt hại về tài sản, khi một hệ thống bị tê liệt thì sẽ hệ lụy đến nhiều hoạt động hay giao dịch của hệ thống đó.

Từ khi ra đời kỹ thuật tấn công từ chối dịch vụ cho đến nay đã có rất nhiều các cuộc tấn công dựa trên phương thức này, và củng xảy xa rất nhiều cuộc tấn công đình đám, khiến các ông lớn như Google hay Facebook củng dính phải.

Nguồn tài liệu tham khảo:

1. [http://vi.wikipedia.org](http://vi.wikipedia.org/wiki/T%C6%B0%E1%BB%9Dng_l%E1%BB%ADa)
2. [http://www.quantrimang.com.vn](http://www.quantrimang.com.vn/firewall-cac-khai-niem-tinh-chat-nguyen-ly-va-su-dung-firewall-23)
3. [https://nguyentanvy.wordpress.com](https://nguyentanvy.wordpress.com/2011/11/28/cc-thnh-ph%E1%BA%A7n-c%E1%BB%A7a-firewall-v-c%C6%A1-ch%E1%BA%BF-ho%E1%BA%A1t-d%E1%BB%99ng/)
4. <http://congdd.wordpress.com>
5. <http://exploitx.org>