CHƯƠNG 8: MỘT SỐ VẤN ĐỀ VỀ AN NINH HỆ THỐNG

8.1. Kẻ xâm nhập

8.1.1. Khái niệm

Vấn đề quan trọng đối với hệ thống mạng là chống lại việc truy cập không mong muốn qua mạng máy tính lớn hoặc cục bộ. Chúng ta có thể phân loại kẻ xâm nhập như sau:

- Kẻ giả danh: người không có quyền sử dụng hệ thống, vượt qua kiểm soát truy cập lợi dụng tài khoản người sử dụng hợp pháp.
- Kẻ lạm quyền: là người sử dụng hợp pháp, nhưng truy cập dữ liệu, chương trình hoặc tài nguyên mà không có quyền hoặc là người có quyền truy cập đó nhưng lạm dụng đặc quyền của anh ta.
- Người sử dụng giấu mặt: là người lạm dụng quyền kiểm soát tối cao của hệ thống để vượt qua sự kiểm tra và kiểm soát truy cập hoặc ngăn chặn mọi bản ghi kiểm tra.

Có nhiều mức độ về khả năng xâm nhập khác nhau. Rõ ràng vấn đề trên được công khai và trở nên bức xúc từ sự kiện nổi tiếng "Wily Hacker" trong năm 1986-1987, dẫn đến việc thành lập ngày càng nhiều các đội ứng cứu tình trạng khẩn cấp của máy tính.

Với đội ứng cứu có thể cảm thấy yên tâm hơn nhưng đòi hỏi các nguồn chi bổ sung để phát triển và duy trì hoạt động. Kẻ xâm nhập có thể sử dụng các công cụ làm hại để tấn công các hệ thống.

8.1.2. Các kỹ thuật xâm nhập

Mục tiêu của kẻ xâm nhập là dành quyền truy cập hoặc tăng quyền trong hệ thống. Các phương pháp tấn công cơ bản bao gồm

- Tìm mục tiêu và thu thập thông tin;
- Thực hiện được việc truy cập ban đầu;
- Sau đó tìm cách leo thang quyền.
- Đặc biệt tìm cách nắm bắt file mật khẩu người sử dụng.

Mục tiêu chính là lấy được mật khẩu và sau đó dùng quyền truy cập của người sở hữu.

8.1.3. Đoán mật khẩu

Đoán mật khẩu là một trong các hướng tấn công chung nhất. Kẻ tấn công đã biết tên người sử dụng đăng nhập (từ trang email/web) và tìm cách đoán mật khẩu.

- Mặc định, mật khẩu ngắn, tìm kiếm các từ chung. Nhiều người không thay đổi mật khẩu sau khi được trao tài khoản.
- Thu thập thông tin của người dùng (thay đổi tên, ngày sinh, số điện thoại, các mối quan tâm và từ chung).
- Tìm kiếm tổng thể mọi khả năng có thể của mật khẩu.

Kẻ xâm nhập kiểm tra đăng nhập với tệp mật khẩu đánh cắp được. Sự thành công của việc đoán mật khẩu phụ thuộc vào mật khẩu được chọn bởi người dùng. Tổng quan chỉ ra rằng nhiều người sử dụng chọn mật khẩu không cẩn thận.

Nắm bắt mật khẩu

Tấn công khác bao gồm việc nắm bắt mật khẩu thông qua

- Theo dõi qua vai khi nhập password.
- Sử dụng chương trình ngựa thành Toroa để thu thập thông tin về mật khẩu.
- Theo dõi login mạng không an toàn, chẳng hạn Telnet, FTP, Web, email.
- Chắt lọc thông tin ghi lại sau lần vào mạng được thành công (đệm/lịch sử web, số quay cuối,…).

Người sử dụng cần được học để dùng các biện pháp phòng và ngăn ngừa thích hợp.

8.1.4. Phát hiện xâm nhập

Khi có kẻ xâm nhập vào hệ thống, chắc chắn có lỗi an toàn ở đâu đó, như vậy để phát hiện xâm nhập cần phải:

- Chia khối nguồn tài nguyên để phát hiện nhanh khu vực có kẻ xâm nhập.
- Thực hiện ngay các hành động ngăn chặn để hạn chế tối đa tổn hại.
- Thu thập thông tin định danh kẻ xâm nhập để có biện pháp tăng cường an ninh.
- Giả thiết rằng kẻ xâm nhập sẽ hành động khác so với người dùng hợp pháp. Nhưng sẽ chỉ có sự khác biệt nhỏ giữa họ.

Các cách tiếp cận phát hiện xâm nhập

Phát hiện dựa trên các thống kê bất thường:

- Vượt qua ngưỡng thống kê nào đó của các sự kiện.
- Dựa trên hồ sơ hành vi của người sử dụng để phát hiện những hoạt động bất thường.

Dựa trên quy tắc

- Phát hiện hành động bất thường dựa trên quy tắc được xây dựng từ các mẫu sử dụng trước.
- Định danh thâm nhập: sử dụng các hệ chuyên gia để tìm kiếm các hành động nghi ngờ.

Các bản ghi kiểm tra

Công cụ cơ bản để phát hiện xâm nhập là các bản ghi kiểm tra. Bản ghi về hành động hiện tại của người sử dụng được duy trì như đầu vào của hệ thống phát hiện.

Một phần của hệ điều hành đa người sử dụng đã có công cụ thu thập thông tin về hoạt động của người sử dụng, nên nó đã sẵn sàng để sử dụng. Nhưng nó có nhược điểm là có thể không có thông tin cần thiết và không chứa trong định dạng mong muốn.

Có thể sử dụng các bản ghi kiểm tra chuyên dùng để phát hiện. Nó được tạo ra để thu thập một số thông tin mong muốn, tuy nhiên phải trả giá cho chi phí bổ sung trong hệ thống.

Phát hiện thống kê bất thường

Chủ yếu dùng phương pháp thống kê để phát hiện ngưỡng như:

- Đếm sự xuất hiện của sự kiện đặc biệt theo thời gian.

- Nếu nó vượt quá giá trị nào đó thì cho là đã có kẻ xâm nhập.
- Nếu chỉ dùng nó thì đây là phát hiện thô không hiệu quả.

Có thể kết hợp thống kê với việc dựa trên hồ sơ của người sử dụng:

- Đặc trưng hành vi quá khứ của người sử dụng.
- Phát hiện các hệ quả quan trọng từ hồ sơ đó.
- Mô tả các hồ sơ bằng nhiều tham số khác nhau.

Phân tích bản ghi kiểm tra là cơ sở của cách tiếp cận thống kê. Nó dùng để nhận được các số liệu thống kê theo thời gian:

- Số đếm, đo, thời gian khoảng, sử dụng nguồn. Dùng các bản ghi kiểm tra khác nhau trên số liệu phân tích để xác định hành vi hiện tại có chấp nhận được không.
- Tính kỳ vọng, phương sai của các biến nhiều chiều, chuỗi thời gian để rút ra các kết luận thống kê.

Ưu điểm chính là không cần sử dụng kiến thức biết trước để phát hiện.

Phát hiện xâm nhập dựa trên quy tắc

Quan sát các sự kiện trong hệ thống và áp dụng các quy tắc để quyết định hoạt động đó có đáng nghi ngờ hay không. Phát hiện bất thường dựa trên quy tắc được tiến hành như sau:

- Phân tích các bản ghi kiểm tra cũ để xác định mẫu sử dụng và đưa ra quy tắc tự sinh cho chúng.
- Sau đó quan sát hành vi hiện tại và sánh với các quy tắc để nhận thấy nếu nó phù hợp.
- Giống như phát hiện thống kê bất thường không đòi hỏi kiến thức biết trước về các lỗi an ninh.

Định danh sự thâm nhập dựa vào quy tắc có cách tiếp cận sử dụng công nghệ hệ chuyên gia.

- Các đặc trưng chính của các hệ thống này là đưa ra quy tắc định danh sự xâm nhập khai thác các điểm yếu đã biết, hoặc các hành vi nghi ngờ;
- Rồi so sánh các bản ghi kiểm tra hoặc các trạng thái theo quy tắc;
- Quy tắc được sinh bởi các chuyên gia, những người đã phỏng vấn và hệ thống các kiến thức của các quản trị an ninh.
- Chất lượng phụ thuộc vào cách thức thực hiện các nguyên tắc trên.

Ảo tưởng phát hiện dựa trên tỷ lệ

- Trên thực tế để sử dụng cần phát hiện kẻ xâm nhập hệ thống với tỷ lệ đúng cao với tỷ lệ rất nhỏ các cảnh báo sai. Hai tỷ lệ này cần phải được cân đối cho từng hệ thống:
  - Nếu rất ít sự xâm nhập được phát hiện, suy ra an ninh không tốt.
  - Nếu rất nhiều cảnh báo sai, khi đó phí thời gian để kiểm tra xem xét.
- Điều trên nói chung rất khó thực hiện nó tùy thuộc vào yêu cầu an ninh của hệ thống.
- Các hệ thống hiện nay dường như chưa có các bản ghi kiểm tra tốt.

Phát hiện xâm nhập phân tán

Các hệ thống thông tin truyền thống thường tập trung, đơn lẻ. Nhưng ngày nay thông thường các hệ thống máy tính đều lớn và gồm nhiều máy chủ phân tán. Do đó việc phát hiện kẻ xâm nhập vào hệ thống rất khó khăn. Muốn bảo vệ hiệu quả cần làm việc cùng nhau để phát hiện kẻ xâm nhập. Các vấn đề đặt ra cần giải quyết là:

- Làm việc với nhiều định dạng bản ghi kiểm tra khác nhau, trên nhiều hệ điều hành khác nhau.
- Toàn vẹn và bảo mật dữ liệu trên mạng, kể cả trên đường truyền Internet.
- Kiến trúc bây giờ là phân tán, các máy chủ bố trí xa nhau trong phạm vi rộng lớn.
- Cần phải kết hợp sử dụng module tác tử máy chủ, module tác tử giám sát mạng LAN và module quản trị trung tâm để cùng nhau phát hiện và đưa ra biện pháp phòng chống.

Sử dụng bình mật ong

- Chăng lưới thu hút các kẻ tấn công.
  - Tách khỏi sự truy cập đến các hệ thống then chốt;
  - Để thu thập các thông tin về hoạt động của chúng;
  - Kích thích kẻ tấn công ở lại trong hệ thống để người quản trị có thể phán đoán.
- Được cấp đầy đủ các thông tin bịa đặt.
- Được trang bị để thu thập chi tiết thông tin về hoạt động của kẻ tấn công.

8.2. Quản trị mật khẩu

Quản trị mật khẩu là bảo vệ tuyến đầu chống kẻ xâm nhập. Người sử dụng được cung cấp cả hai thông tin:

- Login – xác định đặc quyền của người sử dụng;
- Password – xác thực danh tính của người sử dụng.

Cần phải bảo vệ file mật khẩu trong hệ thống và nó thường được lưu trữ dạng mã hóa hoặc dạng bản băm:

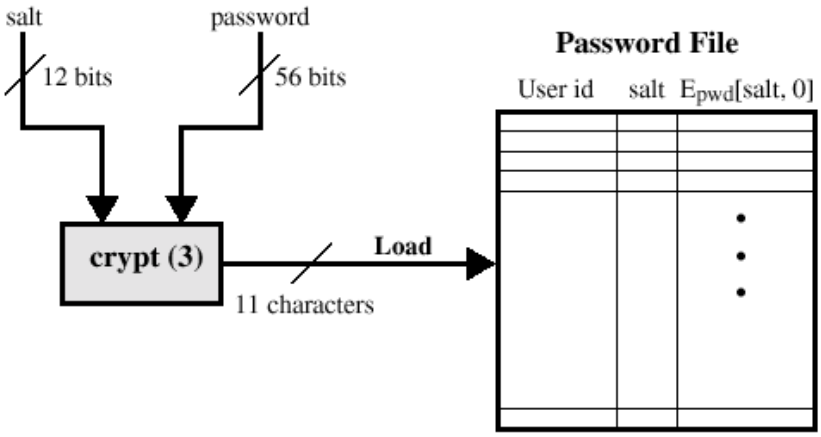
- Unix sử dụng DES lặp để lưu mật khẩu.
- Các hệ thống gần đây sử dụng hàm hash để băm mật khẩu và lưu bản băm. Đặc biệt có thể dùng bản băm làm khóa mật sinh ra từ mật khẩu.

Lỗ hổng mật khẩu.

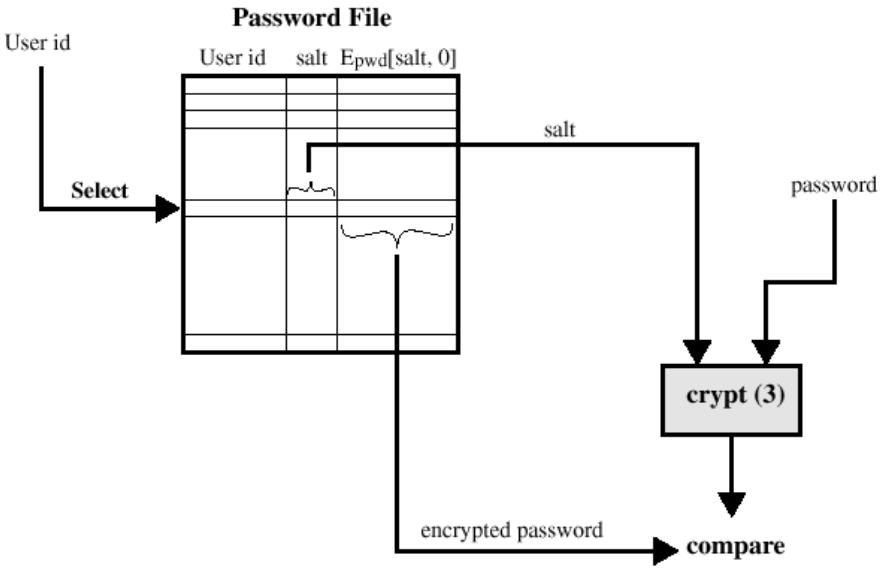
Để hiểu về bản chất mối đe dọa hệ thống mật khẩu, ta xét sơ đồ được áp dụng rộng rãi trên Unix, ở đó mật khẩu không bao giờ lưu trữ dạng tường minh.

Mỗi người sử dụng chọn mật khẩu dài đến tám ký tự in được, nó chuyển thành 56 bit (sử dụng 7 bit ASCII) và là đầu vào chính cho cơ chế mã hóa crypt(3) dựa trên DES. Thuật toán DES được biến thể sử dụng 12 bit "muối" bổ sung. Giá trị này thường liên quan đến thời điểm mà mật khẩu được chọn bởi người sử dụng. Thuật toán đó sử dụng khối dữ liệu gồm 64 bit 0. Đầu ra của nó lại là đầu vào của thuật toán mã hóa lần 2. Quá trình lặp lại 25 lần. Đầu ra cuối 64 bit được chuyển thành dãy 11 ký tự. Bản mã mật khẩu được lưu cùng với bản rõ của "muối" trong file mật khẩu tương ứng với ID của người sử dụng.

"Muối" có tác dụng làm cho mật khẩu không bị lặp, tăng độ dài mật khẩu và tránh dùng cài đặt DES trên phần cứng.



Khi đăng nhập vào hệ thống Unix, người sử dụng cung cấp định danh và mật khẩu. Hệ điều hành sử dụng định danh lấy bản rõ "muối" và bản mã mật khẩu. Sau đó dùng "muối" và mật khẩu tạo thành bản mã mật khẩu rồi sánh với giá trị lưu và quyết định mật khẩu chấp nhận hay không.
Có hai mối đe dọa hệ mật khẩu Unix. Người sử dụng giành quyền truy cập hệ thống bằng cách đoán tài khoản và chạy chương trình đoán mật khẩu. Hơn nữa, nếu có bản copy file mật khẩu, kẻ tin tặc có thể chạy chương trình đăng nhập trên máy khác để tăng tốc độ dò tìm.



Khóa mật sinh từ mật khẩu (trong sơ đồ Kerberos).

Các ký tự mật khẩu có thể biểu diễn theo định dạng 7 bit của ASCII. Mật khẩu với độ dài tùy ý sẽ được biến đổi thành khóa mật:

- Trước hết, xâu mật khẩu s được lưu dạng các ký tự 7 bit, sau đó cuộn gọn lại nhờ phép XOR thành 56 bit.
- Lấy nó làm 56 bit khóa của DES, bổ sung thành 64 bit khóa gồm 8 khối 8 bit.
- Mật khẩu gốc được mã theo chế độ mã móc nối dây chuyền với khóa được tạo ở trên.
- Kết quả nhận được khóa 64 bit sinh ra từ mật khẩu.

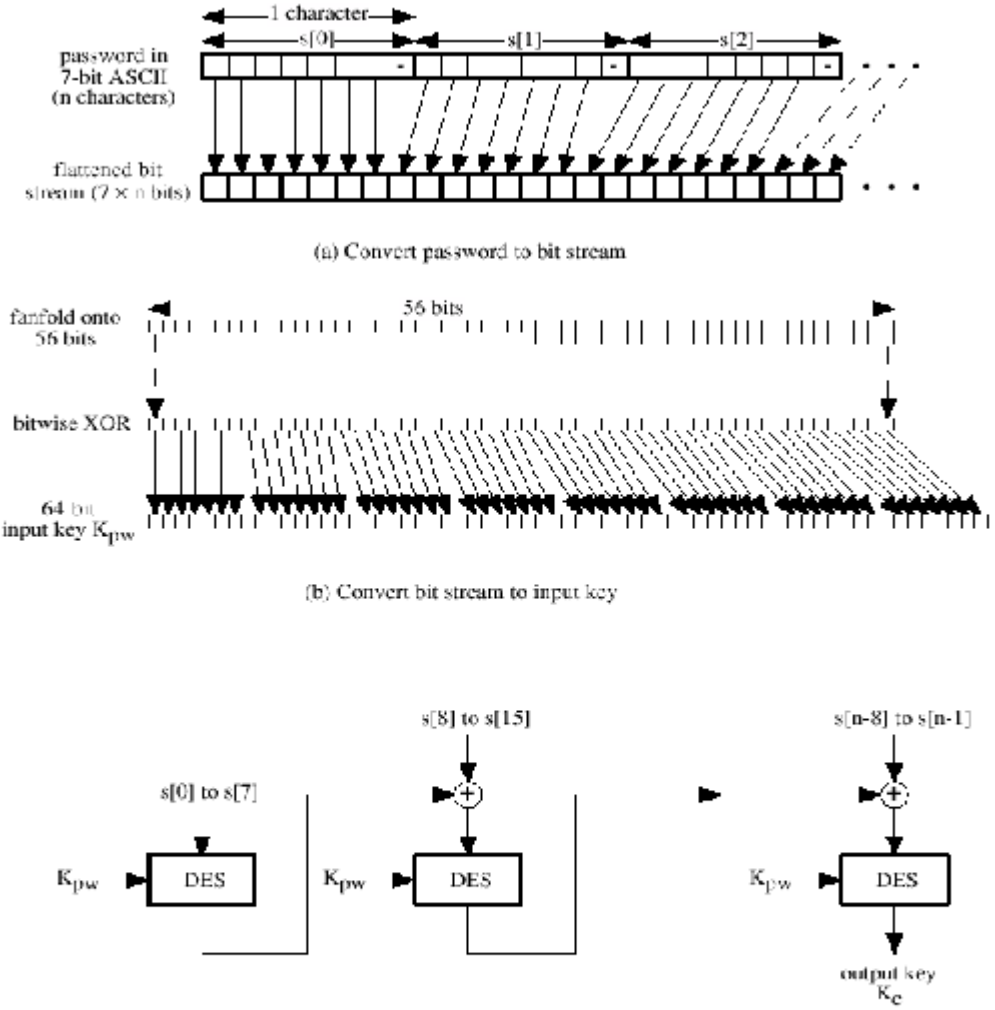


Figure 4.6 Generation of Encryption Key from Password

Tìm hiểu về mật khẩu:

- Theo Purdue năm 1992, có nhiều mật khẩu ngắn.
- Theo Klein năm 1990, có nhiều mật khẩu đoán được.
- Kết luận là người sử dụng thường chọn các mật khẩu không tốt.
- Cần một cách tiếp cận để chống lại điều đó, giúp người sử dụng tạo nên các mật khẩu tốt, khó đoán.

Tạo mật khẩu - cần giáo dục cách tạo mật khẩu:

- Cần có chính sách và giáo dục người sử dụng tạo mật khẩu an toàn.
- Giáo dục tầm quan trọng của mật khẩu tốt.
- Cho định hướng mật khẩu tốt:
    - Độ dài tối thiểu lớn hơn 6.
    - Đòi hỏi trộn chữ hoa và chữ thường, số và dấu chấm.
    - Không chọn các từ có trong từ điển, tức là có ý nghĩa nào đó.
    - Nhưng nên chọn sao cho nhiều người không để ý.

Tạo mật khẩu – máy tính tự sinh:

- Cho máy tính tự tạo mật khẩu một cách ngẫu nhiên theo các tiêu chuẩn tốt.
- Nếu ngẫu nhiên không dễ nhớ thì khi viết sẽ khó khăn (hội chứng nhãn khó chịu)
- Ngay cả phát âm được cũng không thể nhớ mật khẩu được do không có ý nghĩa.
- FIPS PUB 181 là một trong những bộ sinh mật khẩu tốt nhất:
    - Có cả mô tả và code ví dụ.
    - Sinh từ việc ghép ngẫu nhiên các âm tiết phát âm được.

Tạo mật khẩu - kiểm tra trước:

- Đây là cách tiếp cận hứa hẹn nhất để có thể cải thiện an toàn mật khẩu.
- Cho phép người sử dụng chọn trước mật khẩu của mình.
- Nhưng để cho hệ thống kiểm chứng xem nó có chấp nhận được không:
    - Bắt buộc theo quy tắc đơn giản
    - So sánh với từ điển các mật khẩu tồi.
    - Sử dụng mô hình thuật toán Markov hoặc bộ lọc để chống các cách chọn tồi.

8.3. Phần mềm có hại

8.3.1. Các kiểu phần mềm có hại.

Virus máy tính đã được công bố rất nhiều là một trong những phần mềm có hại nhất. Tác động của nó mọi người đều biết, đã được nêu trong các báo cáo và phim ảnh, gây nhiều chú ý hơn là tán thưởng và được quan tâm nhiều để phòng chống.

8.3.1.1. Cửa sau hoặc cửa sập

Điểm vào chương trình bí mật, cho phép những người biết truy cập mà bỏ qua các thủ tục an toàn thông thường. Kỹ thuật này có thể được sử dụng chung bởi những người phát triển và là mối đe doạ khi để trong chương trình sản phẩm cho phép khai thác bởi các kẻ tấn công. Rất khó ngăn chặn trong hệ điều hành, đòi hỏi phải cẩn thận ngay từ khi phát triển xây dựng hoặc thường xuyên cập nhật phần mềm.

8.3.1.2. Bom logic

Đây là một trong những phần mềm có hại kiểu cổ, code được nhúng trong chương trình hợp pháp. Nó được kích hoạt khi gặp điều kiện xác định:

- Có mặt hoặc vắng mặt một số file.
- Ngày tháng/thời gian cụ thể.
- Người sử dụng nào đó.

Khi được kích hoạt thông thường nó làm hỏng hệ thống, biến đổi, xoá file hoặc xóa đĩa, làm dừng máy,…

8.3.1.3. Ngựa thành Tơ roa

Chương trình với các tác động phụ được giấu kín, mà thông thường rất hấp dẫn như trò chơi hoặc phần mềm nâng cấp. Khi chạy thực hiện những nhiệm vụ bổ sung, cho phép kẻ tấn công gián tiếp giành quyền truy cập mà họ không thể thực hiện trực tiếp. Thông thường sử dụng ngựa thành Tơ roa để lan truyền virus/sâu (worm) hoặc cài đặt cửa sau hoặc đơn giản là phá hoại dữ liệu.

8.3.1.4. Zombie

Đây là chương trình bí mật điều khiển máy tính của mạng khác và sử dụng nó để gián tiếp tiến hành các cuộc tấn công. Thông thường nó được sử dụng để khởi động tấn công từ chối các dịch vụ phân tán (DdoS) và khai thác các lỗ hổng trong các hệ thống.

8.3.1.5. Virus

Virus là đoạn code tự sinh lặp đính kèm với code khác như virus sinh học. Cả hai đều lan truyền tự nó và mang đi bộ tải

- Mang theo code để tạo các bản sao của chính nó;
- Cũng như mọi code nó cũng thực hiện nhiệm vụ ngầm nào đó như phá hoại các files hệ thống.

Thao tác của virus

Các giai đoạn của virus:

- Nằm im - chờ sự kiện kích hoạt.
- Lan truyền – lặp sinh ra chương trình/đĩa.
- Kích hoạt - bởi sự kiện để thực hiện bộ tải.
- Thực hiện bộ tải.
- Cụ thể thông thường mang tính chất chuyên biệt của các máy và hệ điều hành. Nó khai thác các điểm yếu của hệ thống.

Cấu trúc Virus

```
program V :=
        {goto main;
        1234567;
        subroutine infect-executable :=       {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567) then goto loop
                else prepend V to file; }
        subroutine do-damage :=  {whatever damage is to be done}
        subroutine trigger-pulled := {return true if condition holds}
        main: main-program :=  {infect-executable;
                if trigger-pulled then do-damage;
                goto next;}
        next:
}
```

Dòng mang nhãn 1234567 ký hiệu file hiện thời đã nhiễm virus chưa, nếu chưa thì nó sẽ được đính vào file. Khi thỏa mãn điều kiện nào đó, nó sẽ tiến hành các hành động phá hủy.

Các kiểu Virus

Có thể phân loại dựa trên kiểu tấn công:

- Virus ăn bám là kiểu truyền thống và cũng chung nhất. Chúng đính kèm vào các file thực thi và nhân bản khi chương trình bị nhiễm thực hiện bằng cách nhiễm sang các file thực thi khác.
- Virus cư trú ở bộ nhớ chính như một phần của chương trình hệ thống thường trú. Chúng lây nhiễm mọi chương trình đang thực thi.
- Virus ở sector khởi động lây nhiễm bản ghi khởi động chính và lan truyền khi hệ thống khởi động từ đĩa có virus.
- Lén lút là dạng virus chủ định được thiết kế ẩn náu tránh phát hiện bởi các phần mềm diệt virus.
- Virus nhiều hình thái và biến hoá. Phát hiện định danh bằng dấu hiệu đặc trưng là không thể.

8.3.1.6. Marco Virus

Marco code đính kèm file dữ liệu, được dịch bởi chương trình sử dụng file và là nguồn lây nhiễm chính.

- Như marco của Word/Excel.
- Sử dụng lệnh tự động và lệnh marco.

Đây là đoạn code độc lập với nền tảng, mọi macro virus đều lây nhiễm sang các file doc của Microsoft Word. Mọi chương trình và hệ điều hành hỗ trợ Word cũng bị lây

nhiễm. Nó dựa vào các macro tự động thực hiện không cần tác động tường minh của người dùng. Thông thường đó là các lệnh mở file, đóng file, bắt đầu ứng dụng. Một khi macro chạy, nó sẽ sao nó sang tài liệu khác hoặc xóa file hoặc gây hỏng hệ thống của người sử dụng.

Virus email

Đây là loại virus lan truyền sử dụng email được đính kèm chứa marco virus như Melissa. Nó thường được kích hoạt khi người sử dụng mở file đính kèm hoặc khi mail được xem sử dụng một tính chất script của tác nhân mail, do đó sẽ lan truyền rất nhanh, thông thường đích là tác nhân mail Microsoft Outlook hoặc tài liệu Word/Excel. Để phòng chống ta cần ứng dụng an ninh và hệ điều hành tốt hơn.

8.3.1.7. Sâu

Đây là chương trình sinh lặp nhưng không có tác động, thường sử dụng việc kết nối mạng để lan truyền từ hệ thống này sang hệ thống khác. Ví dụ như sâu Internet Morris 1988.

- Dẫn đến việc tạo ra các đội ứng cứu khẩn cấp máy tính CERT.
- Dùng đặc quyền phân tán hoặc khai thác các điểm yếu hệ thống.
- Được sử dụng rộng rãi bởi Hackers để tạo zombie PC, kéo theo sử dụng các tấn công khác, đặc biệt từ chối dịch vụ DoS.
- Vấn đề chính là mất sự an toàn của hệ thống kết nối mạng thường xuyên.

Thao tác của sâu

Các giai đoạn của sâu giống như virus:

- Nằm im.
- Lan truyền.
  - Tìm hệ thống khác để tác động.
  - Thiết lập kết nối với hệ thống đích từ xa.
  - Tự sinh lặp mình cho hệ thống từ xa.
- Kích hoạt.
- Thực hiện hành động phá hoại.

8.3.1.8. Sâu Morrris

Sâu Morris là loại sâu cổ điển, được tạo bởi Robert Morris vào 1988, nhằm tới các hệ thống Unix. Ở đây sử dụng một số kỹ thuật lan truyền, như

- Phá mật khẩu đơn giản trong file mật khẩu cục bộ.
- Khai thác lỗ hổng của hệ thống.
- Tìm lỗi cửa sập trong hệ thống mail.
- Mọi tấn công thành công sẽ sinh lặp nó.

Tấn công của sâu đương thời

Làn sóng tấn công của sâu đương thời mới từ giữa 2001 như:

- Code Red - sử dụng lỗ hổng MS IIS:
  - Thử IP ngẫu nhiên cho hệ thống chạy IIS (Internet Information Server).

- Có kích hoạt thời gian cho tấn công từ chối dịch vụ.
- Làn sóng thứ hai tác động đến 360000 máy chủ trong vòng 14 giờ.

- Code Red 2 – cài đặt cửa sập.
- Nimda – cơ chế tác động lặp.
- SQL Slammer – đã tấn công máy chủ MS SQL.
- Sobig – đã tấn công máy chủ proxy mở.
- Mydoom – sâu email có số lượng lớn và có cửa sau.

Công nghệ sâu

Các đặc tính của công nghệ sâu là tấn công đa nền tảng, khai thác nhiều chiều, lan truyền cực nhanh, có nhiều kiểu tác động, biến hóa, cơ động và khai thác zero day (tấn công trước khi người phát triển phần mềm biết về điểm yếu của phần mềm ứng dụng).

8.3.2. Các biện pháp chống Virus

Biện pháp tốt nhất là ngăn ngừa, nhưng nói chung là không thể. Do đó cần phải có một trong nhiều biện pháp sau:

- Phát hiện virus nhiễm trong hệ thống.
- Định danh loại virus nhiễm.
- Loại bỏ khôi phục hệ thống về trạng thái sạch.

Phần mềm chống Virus

Phần mềm thuộc thế hệ đầu tiên:

- Quét sử dụng chữ ký của virus để định danh,
- hoặc phát hiện sự thay đổi độ dài của chương trình.

Phần mềm thuộc thế hệ thứ hai:

- Sử dụng các quy tắc trực quan để phát hiện nhiễm virus.
- Sử dụng mã hash của chương trình để phát hiện sự thay đổi.

Phần mềm thuộc thế hệ thứ ba:

- Chương trình thường trú trong bộ nhớ định danh virus theo hành động.

Phần mềm thuộc thế hệ thứ tư

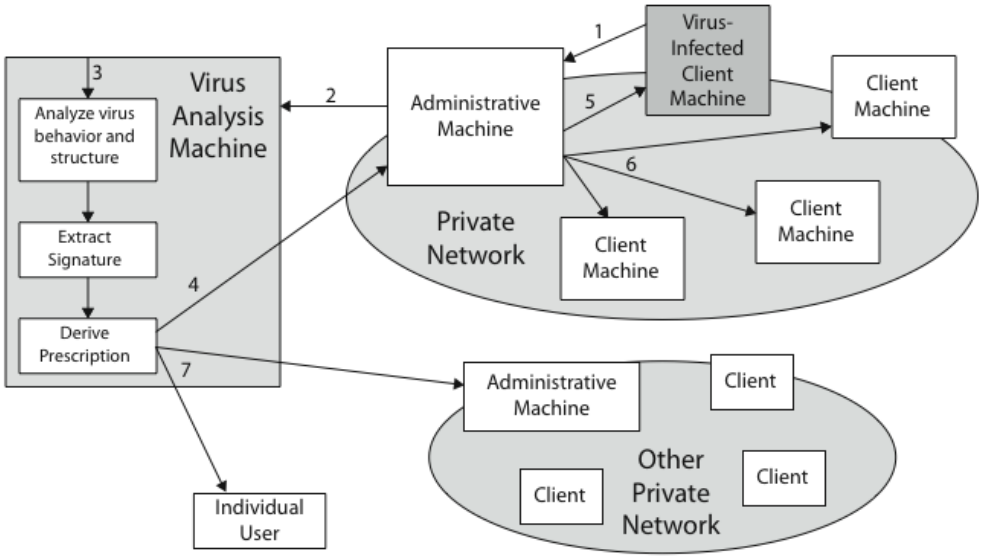
- Đóng gói với rất nhiều kiểu kỹ thuật chống virus
- Quét và lần vết tích cực, kiểm soát truy cập

Phương pháp diệt bằng tay vẫn được dùng.

Kỹ thuật chống Virus nâng cao

- Giải mã mẫu: sử dụng mô phỏng CPU kiểm tra chương trình, chữ ký và hành vi trước khi chạy chúng.
- Dùng Hệ thống miễn dịch số (IBM):
  - Cung cấp việc mô phỏng đa mục tiêu và hệ thống phát hiện Virus.
  - Mọi virus nhập vào tổ chức được nắm bắt, phân tích, phát hiện/tấm chắn tạo ra chống nó và loại bỏ.

Sau đây là sơ đồ Hệ miễn dịch số (Digital Immune System):



Các bước điển hình trong thao tác của hệ miễn dịch là:

- Chương trình giám sát trên mỗi PC sử dụng nhiều kiểu tìm tòi dựa trên hành vi của hệ thống, theo dõi sự thay đổi chương trình hay chữ ký tập thể để phát hiện virus. Sau đó nó gửi bản sao đến máy điều hành.
- Máy điều hành lấy mẫu gửi đến máy phân tích virus trung tâm.
- Máy này tạo môi trường cho máy nhiễm chạy để có thể phân tích. Sau đó nó tạo ra đơn để định danh và loại bỏ virus.
- Đơn được gửi trả lại máy điều hành.
- Máy điều hành gửi lại đơn cho máy bị nhiễm.
- Đơn được gửi tới các máy khác trong tổ chức hệ thống.
- Những người khác ngoài tổ chức sẽ nhận được bản cập nhật chống virus để chống virus mới đó.

8.3.3. Phần mềm ngăn chặn hành vi

Các phần mềm này được tích hợp với hệ điều hành của máy chủ. Chương trình theo dõi các hành vi trong thời gian thực:

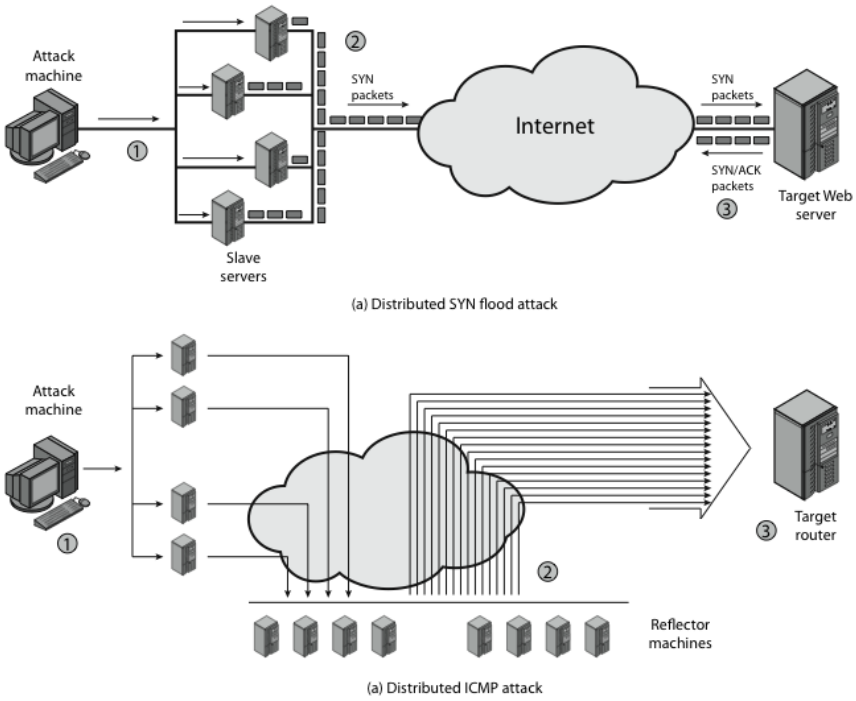
- Chẳng hạn truy cập file, định dạng đĩa, các chế độ thực hiện, thay đổi tham số hệ thống, truy cập mạng.
- Đối với các hành động có khả năng có hại, nếu phát hiện thì ngăn chặn, loại bỏ, trước khi chúng có cơ hội tác động đến hệ thống. Phương pháp này có ưu điểm so với quét, nhưng code có hại chạy trước khi phát hiện.

8.3.3.1. Tấn công từ chối dịch vụ từ xa

Tấn công từ chối dịch vụ từ xa (DDoS) tạo thành đe dọa đáng kể, làm cho hệ thống trở nên không sẵn sàng, làm tràn bởi sự vận chuyển vô ích.

Kẻ tấn công thường sử dụng một số lớn các “Zombies”, tăng độ khó của các tấn công.

Công nghệ bảo vệ tìm các biện pháp đương đầu chống lại



8.3.3.2. Tìm hiểu cách kẻ thù xây dựng mạng lưới tấn công từ chối dịch vụ từ xa

Từ chối dịch vụ có hiệu lực khi bị nhiễm rất nhiều "Zombies". Để thực hiện được điều đó cần có:

- Phần mềm cài đặt tấn công từ chối dịch vụ từ xa.
- Các lỗ hổng không vá được trong nhiều hệ thống.
- Chiến lược quét để tìm lỗ hổng hệ thống: sử dụng các yếu tố ngẫu nhiên, lập danh sách va chạm, tìm hiểu cấu trúc topo, mạng con cục bộ.

8.3.3.3. Chống tấn công từ chối dịch vụ từ xa (DDoS)

Ba cách bảo vệ sau đây được dùng rộng rãi:

- Ngăn ngừa tấn công và chiếm lĩnh trước.
- Phát hiện tấn công và lọc trong quá trình sử dụng dịch vụ.
- Lần vết nguồn tấn công và xác định sự tấn công sau khi sử dụng xong dịch vụ.

Nói chung các khả năng tấn công có phạm vi rộng lớn, vì vậy phải có nhiều biện pháp chống và sử dụng kết hợp chúng.

8.4. Bức tường lửa

8.4.1. Khái niệm

Bức tường lửa phát triển mạnh mẽ, được ứng dụng trong các các hệ thống thông tin. Bây giờ mọi người đều muốn lên Internet và các mạng liên kết với nhau. Vì vậy cần quan tâm thường xuyên về an toàn. Không dễ dàng bảo vệ từng hệ thống trong tổ chức. Thông thường sử dụng bức tường lửa để cung cấp vòng bảo vệ như một phần của chiến lược an ninh toàn diện.

Bức tường lửa là gì

Là điểm cổ chai để kiểm soát và theo dõi thông tin vào ra mạng cục bộ. Các mạng liên kết với độ tin cậy khác nhau, buộc có hạn chế trên các dịch vụ của mạng. Chẳng hạn, vận chuyển phải có giấy phép. Kiểm tra và kiểm soát truy cập, có thể cài đặt cảnh báo các hành vi bất thường. Cung cấp bảng chuyển đổi địa chỉ mạng NAT và sử dụng để theo dõi giám sát. Bức tường lửa có thể được sử dụng để cài đặt mạng riêng ảo (VPN) dùng cơ chế an toàn IPSec.

Hạn chế của bức tường lửa

Không bảo vệ được các tấn công đi vòng qua nó, chẳng hạn mạng lén lút dùng thiết bị modems kết nối ra bên ngoài. Nó ngăn cản cả các tổ chức tin cậy và dịch vụ tin cậy.

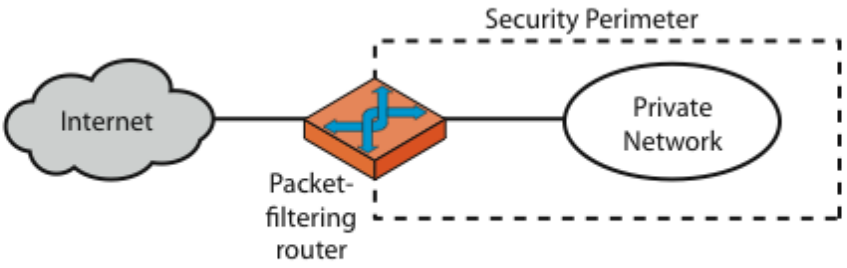
Không bảo vệ chống các mối đe dọa từ bên trong, chẳng hạn như những nhân viên bực tức hoặc thông đồng với kẻ xấu. Không thể bảo vệ chống việc truyền các chương trình hoặc file nhiễm virus, vì các dạng file và các hệ điều hành có phạm vi rất rộng.

8.4.2. Bức tường lửa lọc gói

Là thành phần của bức tường lửa nhanh nhất và đơn giản nhất, là cơ sở của mọi hệ thống tường lửa. Nó kiểm tra mỗi gói IP (không có ngữ cảnh) và cho phép hay từ chối tùy theo quy tắc xác định. Suy ra có hạn chế truy cập đến các dịch vụ và các cổng.

Các đường lối mặc định có thể:

- Default = discard: rằng mọi thứ không cho phép tức là cấm;
- Default = forward: rằng không cấm tức là cho phép.



(a) Packet-filtering router

Bảng sau cho một số quy tắc lọc gói. Trong mỗi tập hợp, quy tắc được áp dụng từ trên xuống dưới. Dấu * trong một trường nào đó là dấu hiệu chỉ ra rằng nó không hạn chế gì cả, sẽ cho phép mọi thứ. Chúng ta giả thiết là Default = discard là chính sách mặc định bắt buộc.

A. Cho phép nhận thư điện tử (cổng 25 dành cho SMTP về), nhưng chỉ đến máy chủ OUR-GW và cổng 25. Tuy nhiên mail từ máy chủ ngoài SPIGOT bị cấm, vì máy chủ có tiến sử không tốt.

B. Ở đây khẳng định tường minh chính sách mặc định Default. Tập quy tắc sẽ bổ sung thêm quy tắc này vào cuối danh sách.

C. Tập quy tắc này mô tả rằng mọi máy chủ bên trong có thể gửi email ra bên ngoài. Gói TCP với cổng đích 25 được định hướng đến máy chủ SMTP trên máy đích. Vấn đề đặt ra là nếu máy chủ bên ngoài được cấu hình để có thể có các ứng dụng khác kết nối với cổng 25. Khi đó kẻ tấn công có thể giành quyền truy cập vào máy bên trong bằng cách gửi gói tin với TCP cổng gốc là 25.

D. Tập quy tắc đạt kết quả mong muốn mà mục C chưa đạt được. Các quy tắc có ưu thế của kết nối TCP. Khi kết nối được thiết lập, cờ ACK của đoạn TCP được thiết lập cho đoạn phúc đáp gửi từ máy bên ngoài. Tập quy tắc khẳng định cho phép các gói IP mà địa chỉ IP gốc là một trong các máy chủ bên trong và số cổng TCP đích là 25. Nó cũng cho phép các gói đến với cổng gốc là 25 mà có cờ ACK trong đoạn TCP.

E. Tập quy tắc này là một trong các cách kiểm soát kết nối FTP. Với FTP, hai kết nối TCP được sử dụng: kết nối điều khiển để khởi tạo việc truyền file và kết nối dữ liệu để truyền file thực tế. Kết nối dữ liệu sử dụng các cổng khác nhau, mà được gán động để truyền. Đa số máy chủ và cũng đa số đích tấn công hoạt động ở các cổng số thấp. Đa số các cuộc gọi ra ngoài hướng tới dùng cổng số cao, thông thường là trên 1023. Như vậy tập quy tắc này cho phép:

- Các gói có gốc từ bên trong;
- Các gói trả lời đến kết nối khởi tạo từ máy bên trong;
- Các gói đến tới các cổng số cao trên các máy bên trong;

Quy tắc E chỉ ra rằng rất khó khi làm việc với các ứng dụng ở mức lọc gói.

Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Các yếu điểm của tường lửa lọc gói

- Tường lửa lọc gói không kiểm tra dữ liệu lớp trên, nên không ngăn chặn các tấn công khai thác lỗ hổng trong các ứng dụng chuyên dụng;
- Đa số lọc gói không hỗ trợ sơ đồ xác thực người dùng nâng cao do thiếu thông tin dữ liệu ở mức cao;
- Dựa trên rất ít biến để quyết định quyền truy cập, nên tường lửa lọc gói dễ nhạy cảm tạo lỗ hổng an ninh do cấu hình không đúng.

Tấn công các lọc gói và các biện pháp phòng chống:

- Địa chỉ IP lừa đảo: giả địa chỉ nguồn làm cho tin tưởng, bổ sung bộ lọc lên mạch chuyển để ngăn chặn.
- Tấn công hướng truyền gốc: kẻ tấn công đặt được hướng truyền khác với mặc định, hy vọng đi vòng qua các kiểm soát an ninh. Biện pháp là loại bỏ mọi gói tin sử dụng lựa chọn này
- Tấn công các đoạn tin nhỏ. Chia thông tin tiêu đề thành một số đoạn nhỏ để lách một số quy tắc dựa trên thông tin tiêu đề. Biện pháp là hoặc bỏ qua các đoạn tin như vậy hoặc sắp xếp lại chúng trước khi kiểm tra.

8.4.3. Bức tường lửa xem xét trạng thái

Lọc gói truyền thống không kiểm tra ngữ cảnh của tầng cao hơn, tức là bức tường lửa lọc gói đơn giản khó hạn chế được các gói đến không mong muốn, tạo ra lỗ hổng được khai thác bởi người sử dụng không có quyền.

Chẳng hạn, giao thức truyền mail cơ bản SMTP cho phép truyền email từ hệ thống máy trạm đến hệ thống máy chủ. Máy chủ sẽ cất chúng trong các hộp thư tương ứng của người sử dụng. SMTP thao tác bằng cách thiết lập kết nối TCP giữa người gửi và máy chủ ở xa với cổng TCP là 25; Số cổng TCP cho SMTP máy trạm nằm giữa 1024 và 16383. Các số nhỏ hơn 1024 giành cho một số ứng dụng riêng biệt. Các số từ 1024 đến 16383 được sinh động và có ý nghĩa tạm thời cho kết nối TCP đó. Lọc gói cơ bản cần phải cho phép các gói đến từ các cổng có số cao cho việc truyền tin dựa trên TCP đã xảy ra. Đây là lỗ hổng mà những người sử dụng không có chủ quyền khai thác.

Bức tường lửa xem xét trạng thái hướng đến yêu cầu khắc phục nhược điểm đó. Chúng kiểm tra mỗi gói IP trong ngữ cảnh: giữ vết theo dõi với các kỳ Client-Server, kiểm tra từng gói có đúng thuộc vào một phiên làm việc không bằng cách tạo ra thư mục cho mỗi kết nối ra bên ngoài. Suy ra có khả năng tốt hơn phát hiện các gói giả tách khỏi ngữ cảnh như chỉ cho phép đến các cổng có số cao là các gói có hồ sơ gắn kết với các thực thể trong thư mục đó.

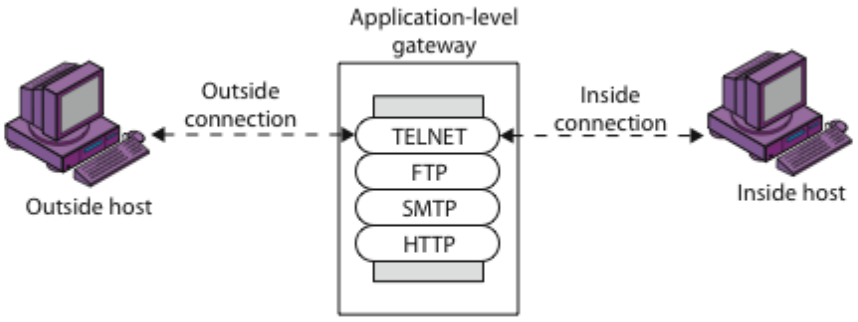
8.4.4. Bức tường lửa – cổng giao tiếp mức ứng dụng (hoặc proxy)

Cổng giao tiếp mức ứng dụng hay còn được gọi là máy chủ proxy hoạt động như tiếp nối vận chuyển mức ứng dụng. Người sử dụng có thể truy cập đầy đủ đến giao thức kết nối:

- Người sử dụng yêu cầu dịch vụ từ proxy;
- Proxy kiểm tra các yêu cầu có hợp lệ không;
- Sau đó xử lý yêu cầu và trả lời cho người sử dụng;
- Có thể vào/theo dõi vận chuyển ở tầng ứng dụng.

Cần các proxies khác nhau cho mỗi dịch vụ:

- Một số dịch vụ hỗ trợ một cách tự nhiên proxy;
- Những loại khác thì cần giải quyết một số vấn đề. Cổng giao tiếp mức ứng dụng hướng tới an toàn hơn lọc gói, có thể cho phép hoặc cấm ở mức TCP và IP. Hơn nữa dễ dàng thực hiện việc đăng nhập và kiểm tra các gói tin đến ở mức ứng dụng.



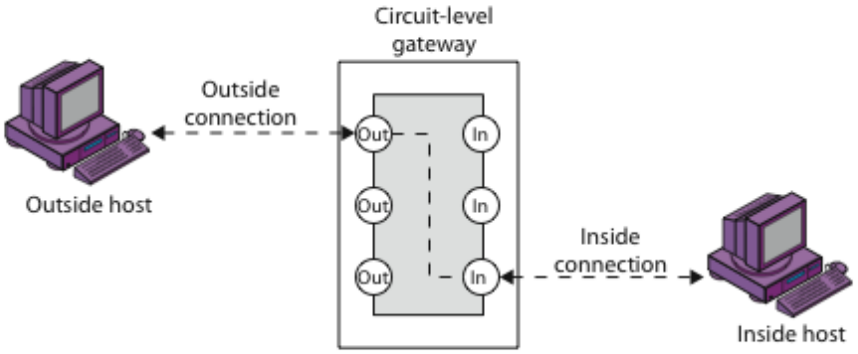
(b) Application-level gateway

8.4.5. Bức tường lửa - cổng giao tiếp mức mạch vòng

Đây có thể là một hệ thống độc lập hoặc một chức năng chuyên dụng của cổng giao tiếp mức ứng dụng. Ở đây không có kết nối TCP đầu cuối, mà cổng sẽ thiết lập chuyển tiếp hai kết nối TCP: một kết nối giữa nó với người sử dụng bên trong và một kết nối giữa nó với người sử dụng bên ngoài. An ninh đạt được bằng cách hạn chế các kết nối này. Mỗi lần tạo ra chuyển tiếp thông thường không kiểm tra nội dung. Nói chung người quản trị tin cậy người sử dụng bên trong bằng cách cho phép các kết nối ra ngoài. Gói SOCKS được sử dụng rộng rãi cho mục đích này, nó được định nghĩa là giao thức được thiết kế cung cấp khung cho các ứng dụng Client/Server để sử dụng các dịch vụ của tường lửa.

Gói SOCKS được định nghĩa trong RFC 1928, nó bao gồm các thành phần sau:

- Máy chủ SOCKS chạy bức tường lửa trên Unix;
- Thư viện SOCKS máy trạm chạy trên máy chủ bên trong bức tường lửa.



(c) Circuit-level gateway

8.4.6. Máy chủ Bastion

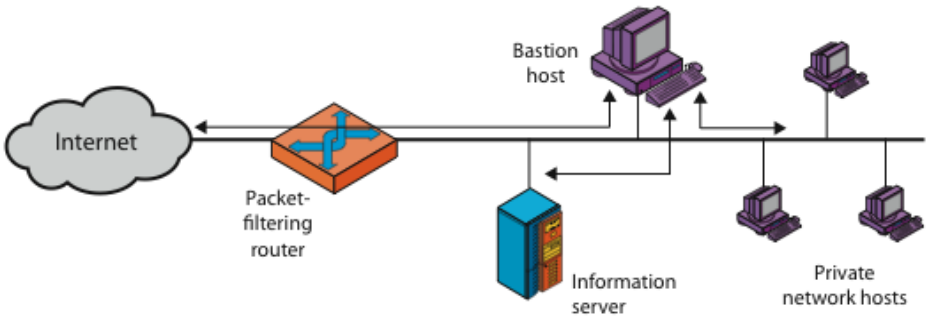
Máy chủ Bastion là hệ thống của người quản trị bức tường lửa, như một điểm rất quan trọng trong an ninh mạng. Thông thường nó là nền tảng cho cổng giao tiếp mức ứng dụng hay mạch vòng. Đó là hệ thống máy chủ an toàn cao.

- Chạy phiên bản an toàn của hệ điều hành, vì an toàn bền vững, nên hệ điều hành nặng nề hơn.
- Chỉ cung cấp các dịch vụ cơ bản bao gồm các ứng dụng proxy như Telnet, hệ thống tên miền DNS, FTP, SMTP và xác thực người sử dụng.
- Máy chủ Bastion có thể yêu cầu xác thực bổ sung trước khi người sử dụng được quyền truy cập các dịch vụ proxy.
- Máy chủ Bastion có tiềm năng thể hiện các yếu tố của máy chủ, các dịch vụ chính, bổ sung xác thực, proxies nhỏ, an toàn, độc lập, không đặc quyền.
- Có thể hỗ trợ hai hay nhiều hơn kết nối mạng và có thể được tin cậy để ép buộc chính sách tách bạch tin cậy giữa các kết nối mạng.

Cấu hình bức tường lửa (Firewall Configurations)

Trong bức tường lửa máy chủ (Screened Host Firewall) chỉ cho các gói tin đến và đi từ các máy chủ Bastion (hình a).

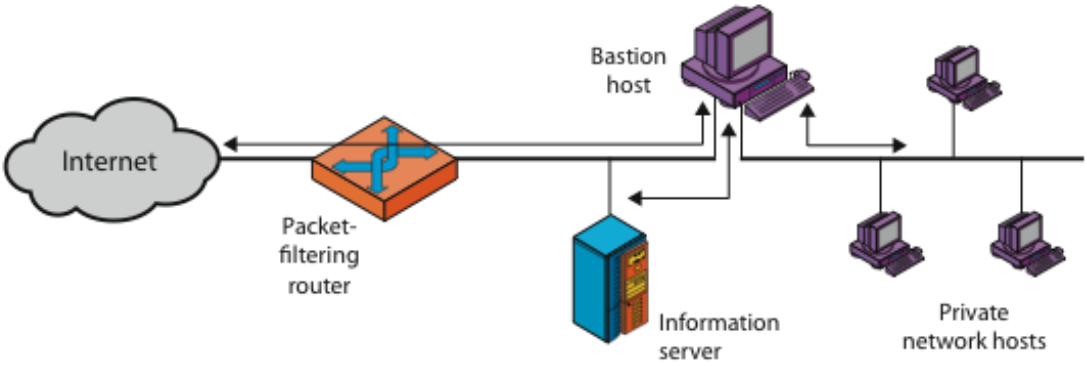
- Ở đó tường lửa gồm 2 hệ thống:
  - Router lọc gói - chỉ cho các gói tin đến và đi từ các máy chủ Bastion;
  - Máy chủ bastion – thực hiện chức năng xác thực và proxy;
- Cấu hình này cung cấp an ninh tốt hơn, vì cài đặt cả lọc mức lọc gói và mức ứng dụng.



(a) Screened host firewall system (single-homed bastion host)

Trong bức tường lửa máy chủ kép (Screened Host Firewall –Dual home): tách bạch hai hệ thống bên trong và bên ngoài (hình b).

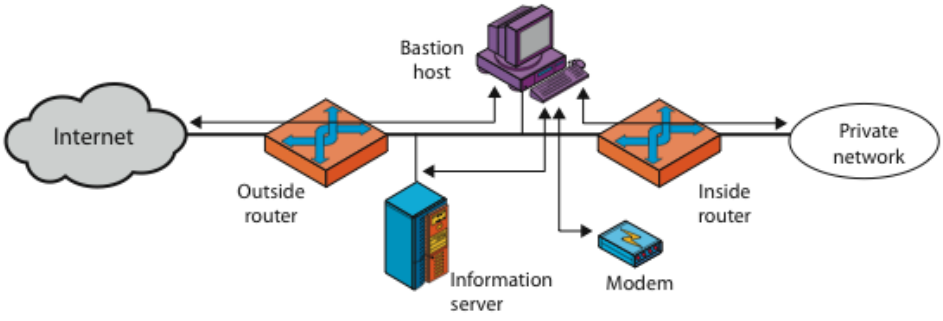
- Máy chủ bastion và máy chủ thông tin có thể liên hệ trực tiếp ra bên ngoài;
- Nhưng mạng cục bộ không liên hệ trực tiếp với bên ngoài, mà thông qua máy chủ bastion.



(b) Screened host firewall system (dual-homed bastion host)

Trong bức tường lửa mạng con (Screened Subnet Firewall) có hai định tuyến lọc gói được sử dụng: một giữa máy chủ Bastion và Internet và một giữa máy chủ Bastion và mạng cục bộ (hình c).

- Ở đây có 3 mức bảo vệ, hai routers và một máy chủ bastion:
  - Bên ngoài không nhìn thấy mạng bên trong.
  - Tương tự bên trong cũng không định tuyến trực tiếp ra bên ngoài
- Máy chủ bastion và máy chủ thông tin có thể liên hệ trực tiếp ra bên ngoài.



(c) Screened-subnet firewall system

8.5. Các hệ thống tin cậy

8.5.1. Kiểm soát truy cập

Hệ thống đã xác định được định danh như người sử dụng, xác định các nguồn gốc nào nó có thể truy cập. Mô hình tổng quát là ma trận truy cập với

- Chủ thể - thực thể chủ động (người sử dụng, quá trình) có khả năng truy cập đối tượng.
- Đối tượng - thực thể bị động (file hoặc chương trình, đoạn trong bộ nhớ) được truy cập đến.
- Quyền truy cập – cách mà đối tượng được truy cập bởi chủ thể.

Có thể được phân tách bởi:

- Cột ứng với đối tượng gồm danh sách quyền truy cập đến nó của các chủ thể định danh.
- Hàng ứng với chủ thể gồm các thẻ về khả năng truy cập của nó đến các đối tượng

Ma trận kiểm soát quyền truy cập

	Program1	...	SegmentA	SegmentB
Process1	Read Execute		Read Execute	
Process2				Read

(a) Access matrix

8.5.2. Khái niệm hệ thống máy tính tin cậy

An toàn thông tin ngày càng quan trọng:

- Có các mức độ khác nhau về sự nhạy cảm của thông tin, phân loại thông tin quân sự: bảo mật, bí mật.
- Chủ thể (người hoặc chương trình) có nhiều quyền khác nhau truy cập đến các đối tượng thông tin.

Được biết như an ninh nhiều tầng:

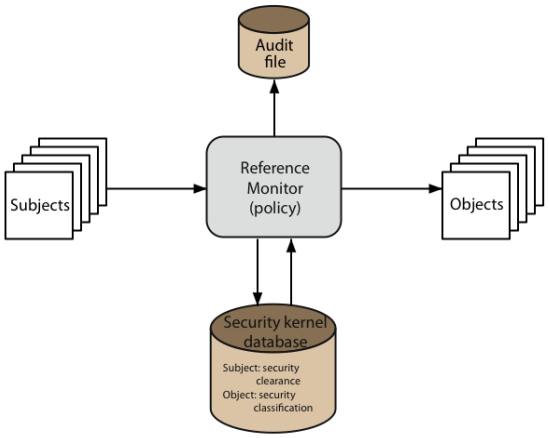
- Chủ thể có các mức độ an ninh thể hiện quyền truy cập.
- Đối tượng có phân loại mức độ an ninh về mặt bảo vệ

Muốn xem xét các cách tăng độ tin tưởng trong hệ thống để củng cố các quyền đó.

8.5.3. Mô hình Bell LaPadula

Mô hình Bell LaPadula là một trong những mô hình an ninh nổi tiếng nhất, được cài đặt như các chính sách bắt buộc trong hệ thống. Có hai chính sách chính

- Không đọc lên (tính chất an ninh đơn giản): chủ thể chỉ có thể đọc các đối tượng nếu mức độ an ninh hiện tại của chủ thể trội hơn phân loại an ninh của đối tượng.
- Không viết xuống: chủ thể chỉ có thể bổ sung/viết lên đối tượng nếu mức độ an ninh hiện tại của chủ thể nhỏ hơn hoặc bằng mức phân loại của đối tượng.



Reference Monitor

(Giám sát truy cập)

8.5.4. Các hệ thống máy tính được đánh giá

Trong khi các hệ thống Công nghệ thông tin phát triển mạnh mẽ, thì có khá nhiều chuẩn đánh giá khác nhau:

- TCSEC, IPSEC và bây giờ là Tiêu chuẩn chung. Xác định một số mức độ đánh giá với việc tăng cường kiểm tra quy tắc. Đã xuất bản danh sách các sản phẩm được đánh giá.
- Chỉ hướng tới sử dụng cho chính phủ/quốc phòng, tuy nhiên cũng có thể hữu ích trong công nghiệp.

Tiêu chuẩn chung

Đặc tả yêu cầu an ninh quốc tế và xác định tiêu chuẩn đánh giá. Tích hợp với các chuẩn khác:

- Chẳng hạn CSEC, ITSEC, CTCPEC (Canada), Federal (US).
- Đặc tả các chuẩn cho việc đánh giá các mức độ an ninh khác nhau.

Tiêu chuẩn đánh giá

- Phương pháp luận cho việc ứng dụng Tiêu chuẩn.
- Các thủ tục hành chính trong việc đánh giá, cấp giấy chứng nhận.
- Xác định tập các yêu cầu an ninh, các mục tiêu đánh giá. Yêu cầu nằm trong hai loại sau, được tổ chức theo các lớp hoặc các thành phần:
  - Chức năng: kiểm soát an ninh, hỗ trợ mã, trao đổi thông tin, bảo vệ dữ liệu người sử dụng, định danh và xác thực, quản lý an ninh, tính riêng tư, bảo vệ các hàm an ninh tin cậy, nguồn thiết thực, đường dẫn tin cậy.
  - Sự tin cậy: quản lý tham số hệ thống, phân phối tham số và thao tác, tài liệu chỉ dẫn, hỗ trợ thời gian sống, kiểm tra, đánh giá lỗ hổng, bảo trì sự tin cậy.

TÓM LƯỢC CUỐI BÀI

Chúng ta đã xem xét:

- Việc phân loại các kẻ xâm nhập vào hệ thống.
- Quản trị mật khẩu.
- Các phần mềm có hại và phòng chống virus.
- Một số mô hình máy tính tin cậy.

CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

1. Mục nào không thuộc phân loại của Kẻ xâm nhập:
   A. Kẻ giả danh
   B. Kẻ xem lén
   C. Kẻ lạm quyền
   D. Người sử dụng giấu mặt
2. Đâu không phải là mục tiêu của kẻ xâm nhập
   A. Nắm bắt mật khẩu người sử dụng hợp pháp
   B. Đăng nhập vào hệ thống để khai thác và phá hoại thông tin
   C. Leo thang tăng quyền truy cập thông tin
   D. Đăng ký thành viên hợp pháp
3. Không dựa vào giả thiết nào để đoán mật khẩu
   A. Mật khẩu ngắn, dễ nhớ
   B. Thông tin cá nhân người sở hữu tài khoản
   C. Mật khẩu dài, ngẫu nhiên, không có ngữ nghĩa
   D. File mật khẩu đánh cắp được hoặc dò tìm mò
4. Mục nào không thuộc việc cần làm để phát hiện kẻ xâm nhập:
   A. Chia khối để phát hiện nhanh
   B. Bảo mật dữ liệu
   C. Hành động ngăn chặn
   D. Thu thập thông tin để tăng cường an ninh
5. Điều nào không đúng trong cách tiếp cận phát hiện hành động bất thường theo ngưỡng:
   A. Đếm sự xuất hiện của sự kiện đặc biệt theo thời gian
   B. Nếu vượt quá giá trị nào đó thì cho là đã có xâm nhập
   C. Nếu chỉ dùng nó thì đây là phát hiện thô không hiệu quả
   D. Theo dõi lý lịch hành vi của người sử dụng đó
6. Điều gì không đúng với việc phát hiện xâm nhập dựa trên mô tả
   A. Đếm sự xuất hiện của sự kiện đặc biệt theo thời gian
   B. Đặc trưng hành vi quá khứ của người sử dụng
   C. Phát hiện hệ quả quan trọng từ đó
   D. Mô tả bằng nhiều tham số
7. Điều gì không đúng với Bản ghi kiểm tra đơn giản:
   A. Một phần của hệ điều hành đa người sử dụng
   B. Sẵn sàng để sử dụng
   C. Có thể không có thông tin trong định dạng mong muốn
   D. Được tạo chuyên dùng để thu thập một số thông tin mong muốn
8. Điều nào không đúng đối với phát hiện dựa trên qui tắc:
   A. Phân tích bản ghi để xác định mẫu sử dụng và qui tắc tự sinh
   B. Quan sát hành vi hiện tại và sánh với các qui tắc
   C. Xác định các tham số ngưỡng tần suất xuất hiện sự kiện
   D. Không đòi hỏi kiến thức biết trước về sai lầm an ninh

9. Điều nào không đúng trong việc định danh kẻ xâm nhập theo qui tắc
   A. Phân tích bản ghi kiểm tra
   B. Sử dụng công nghệ hệ chuyên gia
   C. Dùng các mẫu điểm yếu, hoặc các hành vi nghi ngờ
   D. So sánh các bản ghi kiểm tra hoặc các trạng thái theo qui tắc
10. Điều nào không đúng trong việc thu hút kẻ tấn công
   A. Tách khỏi sự truy cập đến các hệ thống then chốt
   B. Để thu thập các thông tin về hoạt động của chúng
   C. Kích thích kẻ tấn công ở lại trong hệ thống để có thể phán đoán
   D. Giăng bẫy tại các phần quan trọng
11. Điều nào không phải là định hướng mật khẩu tốt
   A. Độ dài tối thiểu > 6
   B. Dựa trên các thông tin cá nhân
   C. Đòi hỏi trộn chữ hoa và chữ thường, số và dấu chấm
   D. Không chọn từ trong từ điển
12. Điều nào không đúng trong việc kiểm tra trước mật khẩu:
   A. Được chọn trước mật khẩu để kiểm tra
   B. Bắt buộc theo qui tắc đơn giản như không dựa vào thông tin cá nhân
   C. So sánh với từ điển các mật khẩu tồi
   D. Thường dùng Từ điển lớn hỗ trợ
13. Điều nào không đúng với phần mềm cửa sập
   A. Điểm vào chương trình bí mật
   B. Cho phép những người biết truy cập mà bỏ qua các thủ tục an toàn
   C. Có thể lây lan sang các hệ thống khác
   D. Là mối đe doạ khi chương trình được khai thác bởi kẻ tấn công
14. Điều nào không đúng đối với Ngựa thành Tơ roa
   A. Chương trình có tác động phụ được giấu kín
   B. Được kích hoạt bởi ngày tháng cụ thể
   C. Thường hấp dẫn như trò chơi, phần mềm miễn phí
   D. Thực hiện nhiệm vụ bổ sung như lan truyền virus, sâu, phá hoại dữ liệu
15. Điều nào không đúng đối với Zombie:
   A. Được kích hoạt bởi chương trình khác
   B. Chương trình bí mật điều khiển máy tính của mạng khác
   C. Dùng để khởi động tấn công từ chối dịch vụ phân tán
   D. Khai thác các lỗ hổng trong hệ thống
16. Điều nào không đúng đối với Virus
   A. Là đoạn code tự sinh lặp đính kèm code khác
   B. Tự nó lan truyền mà mang theo code để tạo bản sao của nó
   C. Thực hiện các hành động ngầm phá hoại
   D. Có thể hoạt động độc lập không cần chương trình khác của máy
17. Điều nào không đúng đối với sâu:
   A. Sinh lặp chủ yếu, có thể có các hành động phụ
   B. Lan truyền trên mạng cực nhanh tấn công từ chối dịch vụ
   C. Cần có chương trình khác của máy để đính kèm
   D. Khai thác các lỗ hổng của hệ thống
18. Đâu không phải là biện pháp hiệu quả phòng chống virus:
   A. Không sao chép chương trình không biết nguồn gốc
   B. Phân tích, ngăn ngừa các phần mềm nghi ngờ, ngăn chặn hành vi
   C. Sử dụng mã hash của chương trình để phát hiện bị nhiễm
   D. Định danh virus, loại bỏ, khôi phục trạng thái sạch

19. Mục nào không phải là cách bảo vệ chống tấn công từ chối dịch vụ:
    A. Ngăn ngừa tấn công và chiếm lĩnh trước
    B. Phát hiện tấn công và lọc trong quá trình
    C. Lần vết nguồn tấn công và định danh tấn công
    D. Xây dựng hệ thống máy tính mạnh đáp ứng mọi yêu cầu
20. Đâu không phải là chính sách của mô hình máy tính an toàn Bell LaPadula
    A. Không đọc lên: chủ thể được đọc các đối tượng có mức an ninh <=
    B. Có nhiều mức độ an ninh cho đối tượng và chủ thể
    C. Không viết xuống: chủ thể được viết lên đối tượng có mức an ninh >=
    D. Chủ thể có mức độ an ninh tối đa và hiện tại, đối tượng có mức an ninh cố định
21. Điều nào không đúng đối với ma trận kiểm soát truy cập
    A. Cột đầu là các chủ thể, hàng đầu là các đối tượng
    B. Các cột như danh sách kiểm soát truy cập đến đối tượng đầu cột
    C. Các hàng như các thẻ về khả năng truy cập của chủ thể đầu hàng
    D. Cột đầu là các đối tượng, hàng đầu là các chủ thể

TRẢ LỜI CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

1. B: Kẻ xem lén là trường hợp riêng của Người sử dụng giấy mặt
2. D: Đăng ký thành viên hợp pháp không phải mục tiêu của kẻ xâm nhập
3. C: Nếu dựa vào giả thiết "mật khẩu dàu, ngẫu nhiên, không ngữ nghĩa" thì việc dò tìm mật khẩu là không khả thi
4. B: Bảo mật dữ liệu không thuộc việc cần làm để phát hiện kẻ xâm nhập
5. D: Đặt ngưỡng không phụ thuộc lý lịch hành vi của NSD.
6. A: Phát hiện xâm nhập dựa trên mô tả không dựa trên việc đếm sự kiện đặc biệt
7. D: Bản ghi kiểm tra đơn giản không chứa các thông tin chuyên dụng
8. C; Phát hiện dựa trên qui tắc không cần xác định ngưỡng tần suất xuất hiện sự kiện
9. A: Định danh kẻ xâm nhập theo qui tắc không dựa trên phân tích bản ghi kiểm tra
10. D: Giăng bẫy tại các phần quan trọng tiềm ẩn rủi ro cao nên không thu hút kẻ tấn công ở đây
11. B: Nếu mật khẩu dựa trên thông tin cá nhân thì sẽ có nguy cơ lộ mật khẩu
12. D: Nếu dùng Từ điển lớn để hỗ trợ kiểm tra trước mật khẩu, thì sẽ rất lâu
13. C: Phần mềm cửa sập là điểm vào chương trình bí mật, nó không lây lan
14. B: Nói chung ngựa thành Tơ roa không kích hoạt bởi ngày tháng cụ thể
15. A: Zombie tự lây lan không cần kích hoạt bởi chương trình khác
16. D: Virus cần đến chương trình khác của máy để kích hoạt, lây lan
17. C: Sâu không cần chương trình khác để đính kèm
18. A: Để phòng chống virus không nên sao chép chương trình không biết nguồn gốc
19. D: Xây dựng hệ thống máy tính mạnh đáp ứng mọi yêu cầu là không khả thi nên không phải là cách bảo vệ chống tấn công từ chối dịch vụ:
20. D: Cần có nhiều mức độ an ninh khác nhau
21. D: Cột đầu là chủ thể và hàng đầu là đối tượng

THUẬT NGỮ TRONG BÀI

- Kẻ xâm nhập: là con người hoặc phần mềm mà truy cập không hợp pháp vào hệ thống máy tính của một tổ chức hoặc cá nhân nào đó
- Bình mật ong: nơi chăng lưới thu hút các kẻ tấn công và tách nơi đó khỏi sự truy cập đến các hệ thống then chốt với mục đích thu thập các thông tin về hoạt động của kẻ tấn công

- Cửa sau hoặc cửa sập là điểm vào chương trình bí mật, cho phép những người biết truy cập mà bỏ qua các thủ tục an toàn thông thường. Kỹ thuật này có thể được sử dụng chung bởi những người phát triển và là mối đe doạ khi có trong chương trình sản phẩm
- Bom logic đây là một trong những phần mềm có hại kiểu cổ, code được nhúng trong chương trình hợp pháp.
- Ngựa thành Tơ roa là chương trình với các tác động phụ được giấu kín, mà thông thường rất hấp dẫn như trò chơi hoặc phần mềm nâng cấp. Khi chạy thực hiện những nhiệm vụ bổ sung, cho phép kẻ tấn công gián tiếp dành quyền truy cập mà họ không thể trực tiếp. Thông thường sử dụng lan truyền virus/sâu (worm) hoặc cài đặt cửa sau hoặc đơn giản phá hoại dữ liệu.
- Zombie đây là chương trình bí mật điều khiển máy tính của mạng khác và sử dụng nó để gián tiếp tiến hành các tấn công. Thông thường sử dụng để khởi động tấn công từ chối các dịch vụ phân tán (DdoS). Nó khai thác các lỗ hổng trong các hệ thống.
- Virus là đoạn code tự sinh lặp đính kèm với code khác như virus sinh học. Nó tự lan truyền mang theo code để tạo các bản sao của chính nó. Và nó cũng thực hiện nhiệm vụ ngầm nào đó như phá hoại các files hệ thống..
- Sâu là chương trình tự sinh lặp và gửi các bản sao lan truyền trên mạng từ hệ thống này sang hệ thống khác. Khi đến nơi mới nó có thể tự kích hoạt sinh tiếp và lan truyền. Nó thực hiện các hành động phá hoại.
- Tấn công lặp là tấn công mà ở đó dịch vụ có chủ quyền đã được thực hiện xong, nhưng bị giả mạo bởi yêu cầu lặp khác để tìm cách sử dụng lại những lệnh có chủ quyền.
- Tấn công từ chối dịch vụ
- là tấn công làm cho hệ thống trở nên không sẵn sàng, làm tràn bởi sự vận chuyển và thực hiện những việc vô ích. Kẻ tấn công thường sử dụng một số lớn các "zombies" để tăng độ khó của các tấn công.

CÁC CÂU HỎI THƯỜNG GẶP

Câu 1. Liệt kê và mô tả ba loại kẻ xâm nhập?
Câu 2. Kỹ thuật chung để bảo vệ file mật khẩu là gì?
Câu 3. Các lợi ích nào đem lại nếu được trang bị hệ thống phát hiện kẻ xâm nhập?
Câu 4. Nêu sự khác biệt giữa phát hiện dựa trên thống kê hành vi bất thường và phát hiện dựa trên qui tắc?
Câu 5. Những đại lượng nào hữu ích cho phát hiện kẻ xâm nhập dựa trên hồ sơ?
Câu 6. Bình mật ong là gì?
Câu 7. Muối là gì trong bối cảnh quản trị khóa Unix?
Câu 8. Liệt kê và mô tả vắn tắt các kỹ thuật chống đoán mật khẩu?
Câu 9. Mô tả một số loại phần mềm có hại?
Câu 10. Mô tả hoạt động của virus đơn giản?
Câu 11. Nêu các pha của thao tác virus và sâu?
Câu 12. Mô tả một số kiểu virus?
Câu 13. Nêu khái quát sâu được lan truyền như thế nào?
Câu 14. Nêu các biện pháp chống virus?
Câu 15. Hệ miễn dịch số là gì?
Câu 16. Giải thích ý nghĩa của ma trận kiểm soát quyền truy cập?

TRẢ LỜI CÁC CÂU HỎI THƯỜNG GẶP

1. Ba loại kẻ xâm nhập
   - Kẻ giả danh: thâm nhập tài khoản hợp pháp
   - Kẻ lạm quyền: tìm cách truy cập trái phép
   - Người sử dụng giấu mặt: tiếm quyền quản trị, giả danh người khác
2. Kỹ thuật chung bảo vệ file mật khẩu:
   - Bổ sung mật khẩu đủ dài và mã hóa
   - Lưu giữ bản băm mật khẩu hoặc khóa sinh từ mật khẩu
3. Lợi ích dùng hệ thống phát hiện kẻ xâm nhập:
   - Kịp thời ngăn chặn
4. Sự khác biệt giữa phát hiện dựa thống kê và qui tắc:
   - Thống kê: không phụ thuộc các lỗ hổng và đặc trưng của hệ thống
   - Qui tắc: dựa vào các đặc trưng của hệ thống, các lỗ hổng
5. Đại lượng hữu ích cho phát hiện dựa hồ sơ: Bản ghi kiểm tra
6. Bình mật ong
   - Lôi kéo kẻ thám mã đến và hoạt động lâu ở đó
   - Tung thông tin giả, ở những nơi không quan trọng
   - Thu thập thông tin về kẻ thám mã, nhận diện
7. Muối trong quản lý mật khẩu của Unix:
   - Độ dài 12 bit bổ sung vào khóa và mã hóa
   - Cho đủ dài và thêm yếu tố ngẫu nhiên không phụ thuộc NSD
8. Các kỹ thuật chống đoán mật khẩu:
   - Tìm mật khẩu tồi, kiểm tra mật khẩu khi đăng ký, so sánh với từ điển mật khẩu tồi
9. Mô tả phần mềm có hại:
   - Cần chương trình máy chủ: cửa sập, bom logic, ngựa thành Tơ roa, virus
   - Độc lập lan truyền: Sâu, Zombie
10. Hoạt động virus đơn giản
    - Đính kèm – nhiễm sang các file
    - Đủ điều kiện thì kich hoạt phá hoại
11. Các pha thao tác của virus và sâu:
    - Nằm in, lan truyền, kích hoạt, thực hiện bộ tải
12. Một số kiểu virus:
    - Ăn bám, cư trú ở bộ nhớ, ở sector khởi động
    - Lén lút, nhiều hình thái, biến hoá
13. Xem bài giảng
14. Xem bài giảng
15. Hệ miễn dịch: sử dụng máy quản trị và máy phân tích phòng chống
16. Ma trận kiểm soát truy cập:
    - Cột gắn với đối tượng được truy cập bởi các chủ thể
    - Hàng gắn với chủ thể: quyền truy cập đến các đối tượng của nó

CÂU HỎI TỰ LUẬN

Câu 1. Hãy phân loại kẻ xâm nhập vào hệ thống và lấy ví dụ minh họa?

Câu 2. Nêu một số kỹ thuật xâm nhập hay được sử dụng?

Câu 3. Việc đoán mật khẩu thường được xảy ra theo những kịch bản nào?

Câu 4. Nêu một số cách tiếp cận để phát hiện kẻ xâm nhập?

Câu 5. Giải thích cách dùng việc kiểm tra và phân tích bản ghi để phát hiện kẻ xâm nhập?

Câu 6. Nêu một số phương pháp phát hiện kẻ xâm nhập dựa trên quy tắc?

Câu 7. Có các biện pháp hỗ trợ nào để tạo mới mật khẩu một cách an toàn?

Câu 8. Bạn hãy nêu nguyên lý tạo khóa từ mật khẩu trong Kerberos 5?

Câu 9. Bạn hãy nêu một số kiểu phần mềm có hại?

Câu 10. Bạn hãy mô tả cấu trúc một chương trình virus?

Câu 11. Nêu các biện pháp chống virus?

Câu 12. Mô tả sơ đồ hệ miễn dịch số? Nêu các bước điển hình trong hoạt động của nó?

Câu 13. Nêu cách chống tấn công từ chối dịch vụ từ xa?

Câu 14. Mô tả ma trận kiểm soát quyền truy cập?

Câu 15. Mô tả hai chính sách chính trong mô hình hệ thống tin cậy Bell LaPadula?

Câu 10. Bức tường lửa là gì? Nêu hạn chế của bức tường lửa.

Câu 11. Mô tả bức tường lửa lọc gói? Điểm yếu điểm của nó và biện pháp phòng chống?

Câu 12. Mô tả hoạt động của bức tường lửa cổng giao tiếp mức ứng dụng và cổng giao tiếp mạch vòng?

Câu 13. Nêu cấu hình của hệ thống máy chủ bức tường lửa Bastion?

BÀI TẬP TRẮC NGHIỆM

1. **Đâu không phải là kiểu của kẻ xâm nhập?**
   A. Kẻ giả danh;
   B. Kẻ lạm quyền;
   C. Người sử dụng giấu mặt;
   D. Người sử dụng hợp pháp.
2. **Mục nào không phải là mục tiêu của kẻ xâm nhập?**
   A. Tìm mục tiêu và thu thập thông tin;
   B. Đọc các thông tin công khai;
   C. Truy cập ban đầu vào hệ thống;
   D. Tìm cách leo thang quyền.
3. **Thao tác nào không phải là tấn công nắm bắt mật khẩu?**
   A. Tìm hiểu các phương pháp tạo nên mật khẩu an toàn;
   B. Khai thác thông tin của người dùng như: họ tên, ngày sinh, số điện thoại, các mối quan tâm và từ chung để đoán mật khẩu;

C. Tìm kiếm tổng thể mọi khả năng của mật khẩu trên cơ sở mật khẩu ngắn của người sử dụng;

D. Đoán mật khẩu qua vai người sử dụng nhập mật khẩu.

4. Hành động nào không phải là để phát hiện kẻ xâm nhập?

A. Chia khối dữ liệu để phát hiện nhanh có kẻ xâm nhập không;

B. Hành động ngăn chặn kẻ xâm nhập tấn công vào hệ thống;

C. Tạo các công cụ hỗ trợ để lựa chọn mật khẩu tốt;

D. Thu thập thông tin để tìm biện pháp tăng cường an ninh.

5. Mục nào không phải là tính chất của Bản ghi kiểm tra cơ bản?

A. Được tạo ra chuyên dụng cho việc phát hiện kẻ xâm nhập;

B. Một phần của hệ điều hành đa người sử dụng;

C. Đã sẵn sàng để sử dụng trong hệ thống;

D. Có thể không có thông tin cần thiết và định dạng mong muốn.

6. Phát hiện bất thường dựa trên quy tắc không có tính chất nào?

A. Phân tích các bản ghi kiểm tra cũ để xác định mẫu sử dụng và tạo quy tắc tự sinh.

B. Quan sát hành vi hiện tại và sánh với các quy tắc để nhận thấy nếu nó phù hợp.

C. Giống như phát hiện thống kê bất thường không đòi hỏi kiến thức biết trước về sai lầm an ninh.

D. Lưu vết bản ghi của các lần truy cập cũ để xem xét đánh giá.

7. Xác định định danh dựa trên các quy tắc không sử dụng tiếp cận nào?

A. Dựa trên các kết quả thống kê;

B. Với quy tắc định danh sự xâm nhập đã biết, các mẫu điểm yếu, hoặc các hành vi nghi ngờ;

C. So sánh các bản ghi kiểm tra hoặc các trạng thái theo quy tắc;

D. Quy tắc được sinh bởi các chuyên gia những người đã phỏng vấn và hệ thống kiến thức của các quản trị an ninh.

8. Đâu không phải là tiêu chuẩn đánh giá lựa chọn mật khẩu?

A. Bắt buộc theo quy tắc đơn giản như độ dài phải đảm bảo, không có mối liên hệ trực tiếp đến tên người sử dụng;

B. So sánh với từ điển các mật khẩu tồi;

C. Sử dụng bộ lọc để chống các cách chọn tồi;

D. Không nên kết hợp chữ với số một cách ngẫu nhiên.

9. Đâu không phải là phần mềm có hại?

A. Cửa sập, Bom logic, Zombie;

B. Giám sát các hành động bất thường;

C. Các loại Virus;

D. Sâu, Ngựa thành Toroa.

10. Đâu không phải kiểu của Virus?

A. Virus ăn bám, Virus cư trú ở bộ nhớ;

B. Virus ở sector khởi động;
C. Virus nhiều hình thái và biến hoá;
D. Virus lan truyền.

11. Thao tác nào không dùng để phát hiện chống virus?

A. Sử dụng các quy tắc trực quan để phát hiện nhiễm virus;
B. Kiểm tra xem xét chương trình trước khi chạy.
C. Sử dụng mã hash của chương trình để phát hiện sự thay đổi;
D. Chương trình thường trú trong bộ nhớ định danh virus theo hành động.

12. Đâu không phải là kỹ thuật chống virus nâng cao?

A. Sử dụng mô phỏng CPU kiểm tra chương trình, chữ ký và hành vi trước khi chạy chúng;
B. Cung cấp mô phỏng đa muc tiêu và hệ thống phát hiện virus.
C. Mọi virus nhập vào tổ chức được nắm bắt, phân tích, phát hiện/tấm chắn tạo ra chống nó và loại bỏ;
D. Sử dụng các quy tắc trực quan để phát hiện nhiễm virus.

13. Đâu không phải là tính chất của phần mềm ngăn chặn hành vi

A. Các phần mềm này được tích hợp với hệ điều hành của máy chủ;
B. Theo dõi hậu quả của các hành vi nghi ngờ;
C. Chương trình theo dõi các hành vi trong thời gian thực: chẳng hạn truy cập file, định dạng đĩa, các chế độ thực hiện, thay đổi tham số hệ thống, truy cập mạng;
D. Đối với các hành động có khả năng có hại: nếu phát hiện thì ngăn chặn, tiêu diệt.

14. Từ chối dịch vụ có hiệu lực khi bị nhiễm rất nhiều "Zombies", để tấn công đạt kết quả đó không cần điều gì sau đây:

A. Phần mềm cài đặt tấn công từ chối dịch vụ từ xa;
B. Các lỗ hổng không vá được trong nhiều hệ thống;
C. Chiến lược quét để tìm lỗ hổng hệ thống: sử dụng các yếu tố ngẫu nhiên, lập danh sách va chạm, tìm hiểu cấu trúc topo, mạng con cục bộ;
D. Xem lén thông tin trên đường truyền.

15. Đâu không phải là cách bảo vệ tấn công từ chối dịch vụ được dùng rộng rãi?

A. Ngăn ngừa tấn công và chiếm lĩnh trước.;
B. Tăng cường khả năng cung cấp dịch vụ của hệ thống máy chủ;
C. Phát hiện tấn công và lọc trong quá trình sử dụng dịch vụ;
D. Lần vết nguồn tấn công và xác định sự tấn công sau khi sử dụng xong dịch vụ.

16. Đối với ma trận truy cập điều gì không đúng?

A. Chủ thể - thực thể chủ động (người sử dụng, quá trình) truy cập đối tượng;
B. Đối tượng - thực thể bị động (file, chương trình hoặc đoạn trong bộ nhớ) được truy cập bởi chủ thể;
C. Quyền truy cập – cách mà đối tượng được truy cập bởi chủ thể được cho trong ma trận;
D. Ma trận không thay đổi theo thời gian.

17. Điều gì không là chính sách chính trong Mô hình Bell LaPadula?

A. Các chủ thể và đối tượng có nhiều mức độ an ninh khác nhau;
B. Không đọc lên: chủ thể chỉ có thể đọc các đối tượng nếu mức độ an ninh hiện tại của chủ thể trội hơn mức độ an ninh của đối tượng;
C. Không viết xuống: chủ thể chỉ có thể bổ sung/viết lên đối tượng nếu mức độ an ninh hiện tại của chủ thể nhỏ hơn hoặc bằng mức độ an ninh của đối tượng;
D. Thao tác đọc viết được cho trong ma trận truy cập.

18. Điều gì không phải là yêu cầu chức năng của Hệ thống máy tính được đánh giá?

A. Kiểm soát an ninh, hỗ trợ mã;
B. Trao đổi thông tin, bảo vệ dữ liệu người sử dụng, định danh và xác thực, quản lý an ninh, tính riêng tư;
C. Quản lý tham số hệ thống, phân phối tham số và thao tác;
D. Bảo vệ các hàm an ninh tin cậy, nguồn thiết thực, đường dẫn tin cậy.

19. Đâu không phải là yêu cầu sự tin cậy của Hệ thống máy tính được đánh giá?

A. Quản lý tham số hệ thống, phân phối tham số và thao tác;
B. Trao đổi thông tin, bảo vệ dữ liệu người sử dụng, định danh và xác thực, quản lý an ninh, tính riêng tư;
C. Tài liệu chỉ dẫn, hỗ trợ thời gian sống của các tham số;
D. Kiểm tra, đánh giá lỗ hổng, bảo trì sự tin cậy.