Câu 21:

Trình bày về vấn đề xâm nhập hệ thống trái phép:

- Khái niệm hành vi xâm nhập hệ thống trái phép, phân loại kẻ xâm nhập (Intruder) theo biện pháp xâm nhập, phân loại Intruder theo hành vi.
- Phát hiện xâm nhập: Mục đích, giả thiết cơ bản trong phát hiện xâm nhập, hai phương pháp tiếp cận trong phát hiện xâm nhập (dựa trên thống kê và dựa trên luật).
- Hệ phát hiện xâm nhập phân tán.

1) Khái niệm hành vi xâm nhập hệ thống trái phép, phân loại kẻ xâm nhập (Intruder) theo biện pháp xâm nhập, phân loại Intruder theo hành vi.

- Khái niệm hành vi xâm nhập hệ thống trái phép: là hành vi xâm nhập vào hệ thống mà mình không được phép truy nhập vào, không được chào đón bởi hệ thống.
- Phân loại kẻ xâm nhập theo biện pháp xâm nhập:
  - Giả mạo: người dùng bất hợp pháp từ bên ngoài xâm nhập vào hệ thống và lợi dụng quyền của một người dùng hợp pháp. (xâm nhập từ bên ngoài)
  - Lạm quyền: người dùng hợp pháp, nhưng sử dụng quyền hạn vượt quá phạm vi cho phép (xâm nhập từ bên trong)
  - Người dùng lén lút: chiếm quyền điều khiển giám sát để tránh khỏi sự kiểm soát và điều khiển truy nhập (thường sử dụng đối với hệ quản trị cơ sở dữ liệu không tốt) (xâm nhập từ bên trong hoặc bên ngoài)
- Phân loại kẻ xâm nhập theo hành vi:
  - Khám phá hệ thống: không có ý định phá hoại, chỉ xâm nhập vào (thử xem khả năng của mình có thể xâm nhập vào được không ^^)
  - Phá hoại: xâm nhập hệ thống và thực hiện các hành vi phá hoại hệ thống (thường là những kẻ trẻ tuổi, hành động nông nổi, thiếu kiến thức, nhiều thời gian rảnh rỗi)

2)Phát hiện xâm nhập: Mục đích, giả thiết cơ bản trong phát hiện xâm nhập, hai phương pháp tiếp cận trong phát hiện xâm nhập (dựa trên thống kê và dựa trên luật).

- Mục đích:
  - Phát hiện nhanh: để tối thiểu hóa thiệt hại và khôi phục hoạt động bình thường cho hệ thống một cách nhanh chóng.
  - Ngăn chặn: hệ thống phát hiện xâm nhập có hiệu quả có thể giúp ngăn chặn các xâm nhập
  - Thu thập thông tin về các kỹ thuật xâm nhập để tăng khả năng ngăn chặn
- Giả thiết cơ bản trong phát hiện hành vi xâm nhập là: hành vi của kẻ xâm nhập trái phép có sự khác biệt so với người dùng hợp pháp và có thể phát hiện được sự khác biệt này. Có thể tiến hành như sau:
  - Phân biệt giữa kẻ giả mạo và người dùng hợp pháp

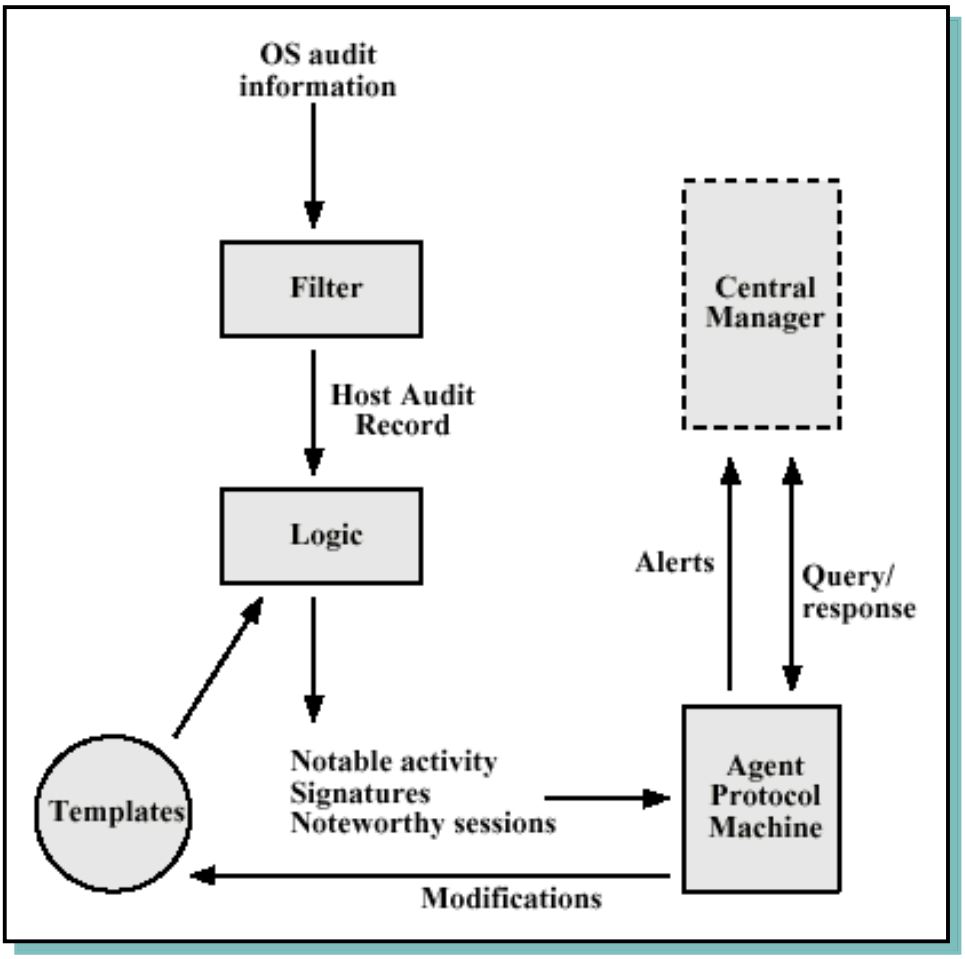
- Quan sát các dữ liệu lịch sử
- Thiết lập các mẫu hình vi
- Quan sát các độ lệch quan trọng trong hành vi

- 2 phương pháp tiếp cận trong phát hiện xâm nhập
  - Phát hiện bất thường theo thống kê:
    - thu thập dữ liệu về hành vi của người dùng hợp pháp trong một khoảng thời gian
    - định kỳ theo dõi các hành vi và xác định hành vi trái phép:
      - dựa vào ngưỡng: tần suất xuất hiện của các sự kiện nhất định
        - Đếm số lần xuất hiện của một kiểu sự kiện nhất định trong một khoảng thời gian
        - Tạo ra cả lỗi tích cực (người dùng thực sự bị coi là kẻ thâm nhập)và lỗi tiêu cực (kẻ xâm nhập trái phép thực nhưng lại không bị coi là kẻ xâm nhập trái phép)
      - dựa trên tiểu sử: từ hồ sơ của hoạt động người dùng, phát hiện ra các thay đổi
        - mô tả hành vi quá khứ của các cá nhân người dùng hoặc các nhóm người dùng có liên quan và sau đó phát hiện ra những sự chênh lệch đáng kể
        - Tiểu sử là một tập các tham số
        - Nền tảng của các tiếp cận này là việc phân tích các bản ghi kiểm soát
        - Các bản ghi qua thời gian định nghĩa hành vi điển hình. Bản ghi kiểm soát hiện thời được dùng để phát hiện sự xâm nhập
    - Không cần hiểu biết trước về khe hở bảo mật
    - cách này thì phát hiện thành công với kẻ xâm nhập giả mạo, còn với kẻ xâm nhập vượt quyền thì khó phát hiện hơn.
  - Phát hiện dựa trên luật
    - quan sát các sự kiện trong hệ thống và áp dụng tập các quy tắc xem hành động có đáng ngờ hay không
    - xây dựng một hệ thống luật xác định hành vi kẻ xâm nhập
      - phát hiện bất thường: phát hiện sự sai khác trong các mẫu hành vi trước đó
        - tự động sinh ra các luật bằng việc phân tích các bản ghi kiểm soát lịch sử để xác định các kiểu sử dụng
        - giả sử tương lai sẽ giống như quá khứ và áp dụng các luật vào hành vi hiện tại
        - không yêu cầu kiến thức về những điểm yếu trong bảo mật
        - cần một cơ sở dữ liệu của các luật lớn (10^4 -> 10^6)
      - nhận diện xâm nhập: hệ chuyên gia tìm kiếm các hành vi đáng ngờ.
        - sử dụng các luật để nhận diện những xâm nhập đã biết hoặc những xâm nhập còn đang nghi ngờ
        - luật được tạo ra bởi các chuyên gia và đặc trưng hệ thống
    - đây là cách tốt hơn so với phát hiện bất thường theo thống kê để phát hiện xâm nhập

3) Hệ phát hiện xâm nhập phân tán

- Phát hiện truy nhập phân tán:
  - Host agent module: quy trình nền thu thập dữ liệu và gửi kết quả tới máy quản lý tập trung
  - Lan monitor agent module: phân tích lưu lượng giao thông trong mạng Lan và gửi kết quả đến máy quản lý tập trung

- Central manager module: xử lý và phối hợp các báo cáo nhận được để phát hiện xâm nhập



- Honeypots:
  - Là các hệ thống giăng bẫy
  - Nhử mồi kẻ tấn công vào những hệ thống quan trọng
  - Thu thập thông tin về kẻ tấn công
  - Giữ kẻ tấn công lại đủ lâu để có thể phản ứng được

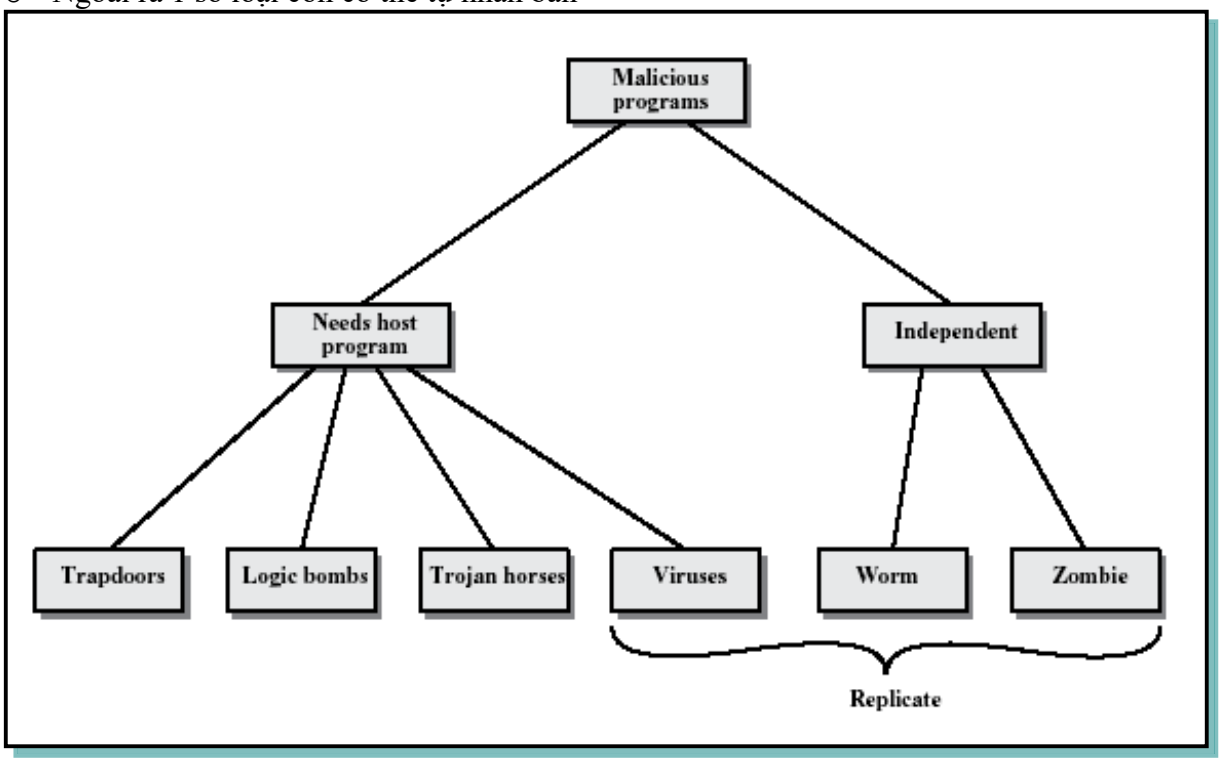
Câu 22:

Trình bày về virus máy tính và các chương trình mã độc:

- Khái niệm, phân loại các chương trình mã độc. Phân biệt virus, sâu (worm), zombie.
- Trình bày cấu trúc chung của một virus, kỹ thuật tránh phát hiện bằng việc nén chương trình chủ.
- Các loại virus (file virus, virus boot sector, virus đa hình, virus macro). Kỹ thuật giải mã họ virus để phát hiện và diệt các virus đa hình.

1) Khái niệm, phân loại các chương trình mã độc. Phân biệt virus, sâu (worm), zombie.

- Khái niệm: chương trình mã độc là một chương trình máy tính hay đoạn mã được thiết kế để gây hại bằng cách phá hủy, tiêu tốn các tài nguyên quý giá, hoặc đặt hệ thống tính toán vào tình trạng không được bảo vệ
- Phân loại: có 2 loại chính
  - Các đoạn mã độc cần một chương trình chủ để ký sinh, coi như một phần của chương trình chủ
  - Chương trình mã độc đứng độc lập
  - Ngoài ra 1 số loại còn có thể tự nhân bản



- Phân biệt virus, sâu (worm), và zombie
  - Viruses: Đoạn mã được nhúng vào chương trình máy tính, và có thể tự nhân bản nó bằng cách gây ra hành động chèn bản sao của nó vào các chương trình khác và thực hiện các hành vi phá hoại. Virus chỉ có thể lây nhiễm khi có sự tác động của người dùng.(*Hành vi chèn bản sao gọi là Lây nhiễm)*
  - Worm: Một chương trình mã độc có khả năng tự nhân bản. Worm sử dụng các kết nối mạng để tự gửi các bản sao của nó qua mạng đến các nút khác mà không cần đến tác động của người dùng (ví dụ gửi chính nó tới tất cả địa chỉ mail trong danh sách …). Không giống virus, worm không cần đến chương trình chủ để ký sinh mà có thể tự tồn tại độc lập.
  - Zombie: Một chương trình chiếm quyền điều khiển một máy tính có nối mạng và sau đó sử dụng máy tính này để thực thi các hành động phá hoại (gửi spam email hoặc dùng để tấn công DDOS).

2) Trình bày cấu trúc chung của một virus, kỹ thuật tránh phát hiện bằng việc nén chương trình chủ.

- Cấu trúc chung của 1 virus:

```
program V:=
```

```
{goto main:
     1234567;// dấu hiệu đặc biệt xác định xem có bị nhiễm chưa

          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 some condition holds}

main:     main-program :=
          {infect-executable;
          if trigger-pulled then do-damage;
          goto next;}
next:// chuyển điều khiển đến chương trình ban đầu

}
```

- Kỹ thuật tránh phát hiện bằng việc nén chương trình chủ
  - Phiên bản bị nhiễm của chương trình dài hơn so với phiên bản gốc (chưa nhiễm)
  - *Giải pháp:* Nén file chương trình -> độ dài chương trình đã nhiễm và chưa nhiễm bằng nhau.

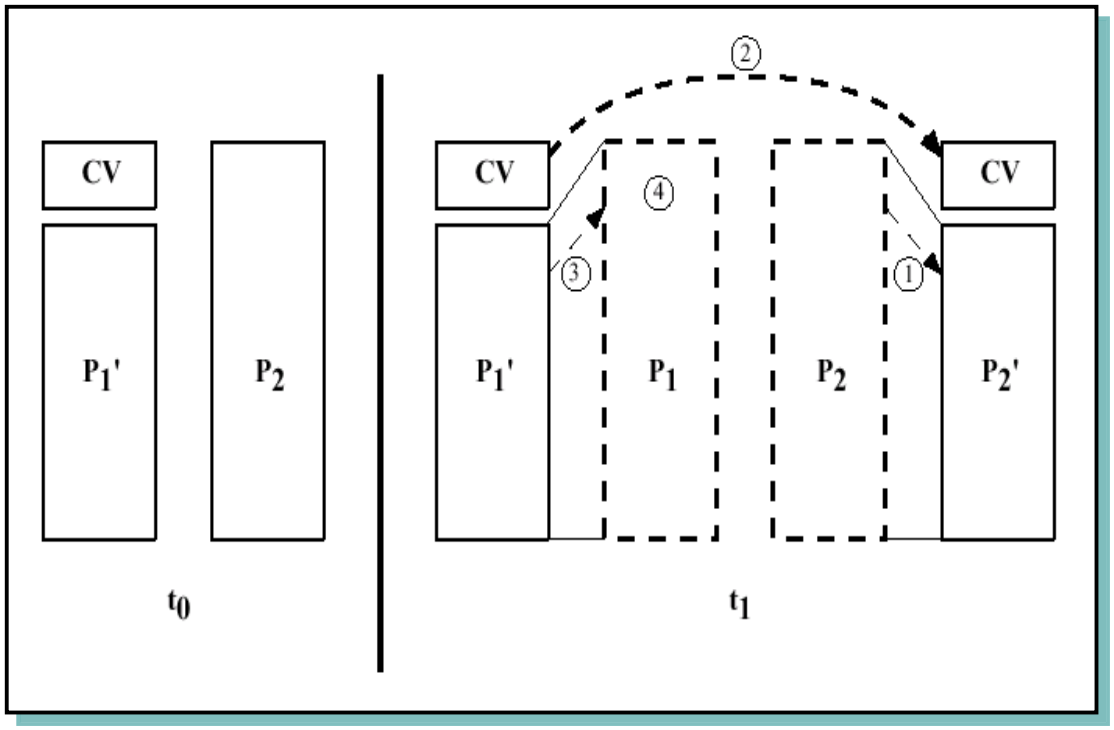
```
        program CV :=

{goto main;
        01234567;

            subroutine infect-executable :=
                        {loop:
                                file := get-random-executable-file;
                        if (first-line-of-file = 01234567) then goto loop;
                (1)     compress file;
                (2)     prepend CV to file;
                }

main:       main-program :=
                        {if ask-permission then infect-executable;
                (3)     uncompress rest-of-file;
                (4)     run uncompressed file;}
                }
```

Chương trình nhiễm virus đã được nén lại có kích thước như chương trình không nhiễm virus không bị nén:



3) Các loại virus (file virus, virus boot sector, virus đa hình, virus macro). Kỹ thuật giải mã họ virus để phát hiện và diệt các virus đa hình.

- Các loại virus:
  - Virus ký sinh: gắn vào các file thực thi, nhân bản khi chương trình được chạy.
  - Virus thường trú bộ nhớ: là một phần của chương trình thường trú bộ nhớ, nhiễm vào tất cả các chương trình được thực thi.
  - Virus boot sector: Nhiễm vào master boot record và lây lan khi hệ thống được khởi động từ đĩa bị virus.
  - Virus giấu mặt: Virus được thiết kế để ẩn mình, tránh bị phát hiện bởi các phần mềm diệt virus (nén, can thiệp các thao tác vào/ra …).
  - Virus đa hình: Loại virus biến đổi sau mỗi lần lây nhiễm (chủ yếu thông qua việc mã hóa chính nó bằng các khóa khác nhau), làm cho việc phát hiện virus qua các mẫu trở nên khó khăn hơn nhiều.
  - Macro virus: Lấy nhiễm các tài liệu Microsoft Word. Chiếm 2/3 số virus hiện có.
- Kỹ thuật giả mã họ virus để phát hiện ra các virus đa hình
  - Dễ dàng phát hiện kể cả các virus đa hình phức tạp nhất.
  - Không ảnh hưởng tới hệ thống
  - Gồm các thành phần sau:
    - Giả lập CPU – phần mềm máy tính ảo
    - Bộ quét nhận diện mẫu virus – quét các chương trình để nhận diện các mẫu virus đã biết
    - Điều khiển giả lập – Điều khiển việc thực thi mã mã độc trong môi trường giả lập.
  - Dựa trên nguyên tắc: Virus đa hình phải tiến hành giải mã thân virus và trao quyền điều khiển cho bộ phận này.
  - Tạo môi trường ảo, trong đó các file bị nhiễm được thực thi mà không ảnh hưởng tới hệ thống.

- Khi các file bị nhiễm thực thi, phần mềm quét sẽ tiến hành rà soát và nhận diện mẫu virus sinh ra.

Câu 23:

Trình bày về firewall:
- Khái niệm, tại sao cần có firewall.
- Các kỹ thuật điều khiển truy cập trong firewall, hạn chế của firewall .
- Các loại firewall: packet-filtering firewall, application-level gateway, circuit-level gateway. Cơ chế hoạt động của từng loại.

1) Khái niệm, tại sao cần có firewall.

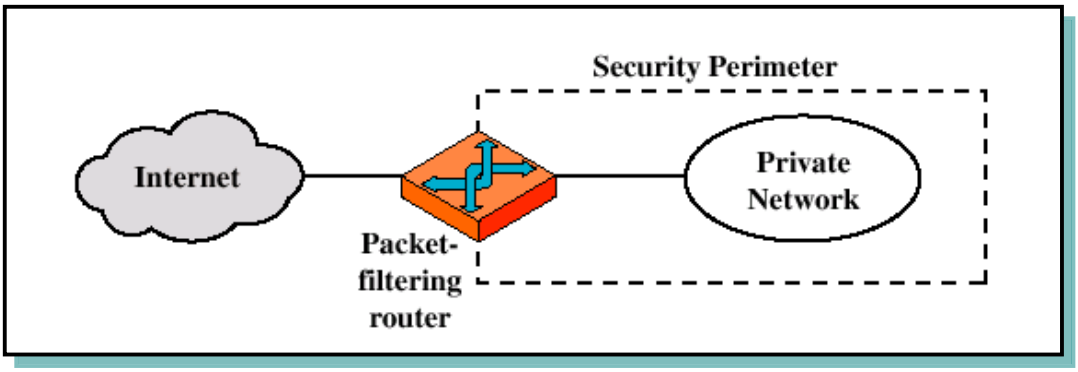
- FireWall là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thông của một số thông tin khác không mong muốn. Nó cũng là một thiết bị hoặc tập các thiết bị được cấu hình để cho phép, từ chối, mã hóa và giải mã tất cả các diao dịch máy tính giữa các miền bảo mật khác nhau dựa trên các quy tắc và tiêu chí.
- Tại sao cần có firewall:
  - Các kết nối Internet cho phép các mạng riêng nối vào hệ thống mạng toàn cầu.
  - Firewall được chèn vào giữa mạng riêng và phần còn lại của Internet.
  - Thiết lập một vành đai bảo vệ và một điểm kiểm soát anh ninh duy nhất.
  - Firewall có thể áp dụng cho một hoặc 1 hệ thống máy chủ.

2) Các kỹ thuật điều khiển truy cập trong firewall, hạn chế của firewall

- Các kỹ thuật điều khiển truy cập trong firewall:
  - Service Control – Điều khiển theo hướng dịch vụ (Internet). Đi vào hoặc ra.
  - Direction Control – Điều khiển theo chiều của dịch vụ.
  - User Control – Điều khiển truy cập dịch vụ theo người dùng.
  - Behavior Control – Điều khiển theo hành vi (các dịch vụ được sử dụng như thế nào)
- Hạn chế của firewall:
  - Không thể chống lại các tấn công bỏ qua firewall (bypass).
  - Không chống lại được các mối đe dọa từ bên trong.
  - Không chống được sự lây nhiễm các chương trình virus và mã độc.

3) Các loại firewall: packet-filtering firewall, application-level gateway, circuit-level gateway. Cơ chế hoạt động của từng loại.

- Packet – filtering firewall:lọc gói tin, kiểm soát từng gói tin một, hoạt động ở tầng mạng, 1 số ở tầng giao vận
  - Áp dụng một tập các luật cho mỗi gói tin đi qua Router và quyết định sẽ chuyển tiếp hay hủy gói tin đó.
  - Lọc gói tin theo *cả hai hướng*



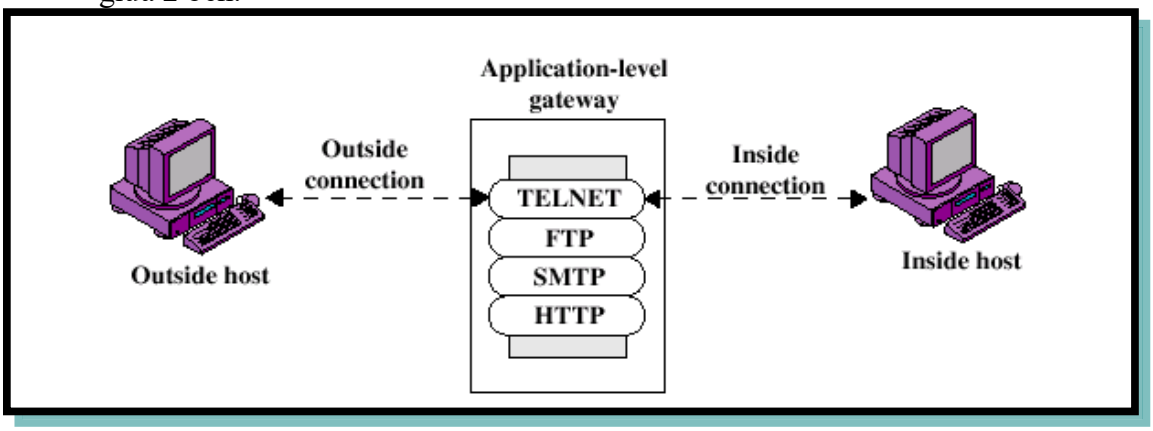
- Các luật dựa trên *địa chỉ nguồn, địa chỉ đích* và *số cổng* để lọc gói tin
- *Danh sách các luật* được khớp với các tham số gói tin.
- Nếu không có luật nào khớp, hành động mặc định được áp dụng.

  Hai chính sách mặc định:

  - default = discard: *Những gói tin không được khai báo rõ ràng là cho qua thì sẽ bị hủy.*

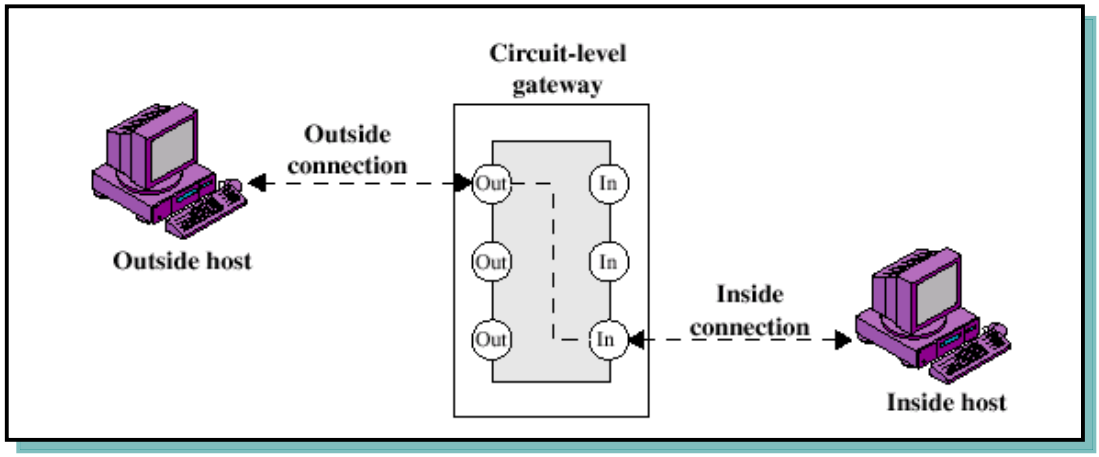
  - default = forward: *Những gói tin không được khai báo rõ ràng là hủy thì sẽ được cho qua.*

- Application-level gateway:
  - Hoạt động như một bộ chuyển tiếp lưu lượng mức ứng dụng.
  - Còn được gọi là máy chủ ủy quyền (proxy)
  - Người dùng kết nối tới gateway để thực hiện TELNET tới máy chủ ở xa, người dùng được chứng thực, sau đó gateway kết nối tới máy chủ ở xa và thông tin được chuyển tiếp giữa 2 bên.



  - Proxy có thể từ chối chuyển tiếp thông tin nếu chứng thực người dùng thất bại hoặc ứng dụng
  - Có thể kiểm tra gói tin qua lại để đảm bảo an toàn - full packet awareness
  - Dễ dàng ghi lại thông tin vì toàn bộ nội dung gói tin có thể hiểu được.
  - *Nhược điểm:* Cần phải thực hiện thêm các xử lý – tăng độ phức tạp xử lý.
- Circuit-level gateway:
  - *Không* cho phép các kết nối TCP end-to-end
  - Thiết lập *hai kết nối TCP*: Một giữa gateway và trạm bên trong, một giữa gateway và trạm bên ngoài.

- *Chuyển tiếp các phân đoạn TCP* từ một kết nối bên này tới kết nối bên kia mà không thực hiện kiểm tra nội dung
- *Chức năng an ninh* (thực hiện theo chính sách) sẽ xác định kết nối nào được phép
- Được dùng khi người dùng bên trong là tin cậy với tất cả các dịch vụ bên ngoài.
- Thường được sử dụng kết hợp với một proxy cho các dịch vụ bên trong.
- Chủ yếu dùng để che giấu thông tin của các mạng riêng bên trong.



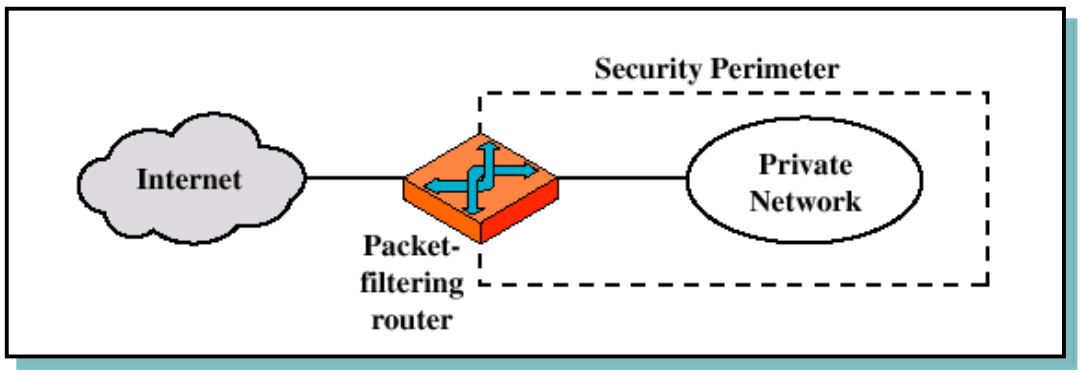
Câu 24:

Trình bày về packet-filtering firewall:

- Khái niệm, cơ chế, ưu nhược điểm của packet-filtering firewall.
- Các biện pháp thường được sử dụng để tấn công packet-filtering firewall: IP Spoofing, Source routing attack, Tiny fragment attack.
- Stateless và Stateful firewall. Ưu điểm của Stateful firewall so với Stateless firewall.

1) Khái niệm, cơ chế, ưu nhược điểm của packet-filtering firewall.

- Khái niệm: packet-filtering firewall là phần mềm tường lửa dựa trên router hoặc chạy thông qua máy tính được cấu hình để giám sát các gói đến và đi.
- Cơ chế:
  - Áp dụng một tập các luật cho mỗi gói tin đi qua Router và quyết định sẽ chuyển tiếp hay hủy gói tin đó.
  - Lọc gói tin theo *cả hai hướng*



- Các luật dựa trên *địa chỉ nguồn, địa chỉ đích* và *số cổng* để lọc gói tin
- *Danh sách các luật* được khớp với các tham số gói tin.
- Nếu không có luật nào khớp, hành động mặc định được áp dụng.

  Hai chính sách mặc định:

  - default = discard: *Những gói tin không được khai báo rõ ràng là cho qua thì sẽ bị hủy.*

  - default = forward: *Những gói tin không được khai báo rõ ràng là hủy thì sẽ được cho qua.*
- Các luật của packet filtering:

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

- Cho phép gửi mail vào (port 25), nhưng chỉ được gửi cho gateway
- Không cho phép lưu lượng đến từ máy SPIGOT

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

- Chính sách *mặc định*
- Luôn luôn là luật cuối cùng
- Luật này cấm tất cả các lưu lượng khác

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

- Các trạm trong mạng có thể gửi mail ra ngoài
- Một vài ứng dụng có thể kết nối tới cổng 25
- Hacker có thể truy cập qua cổng 25

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

- Cải tiến trường hợp trước
- Các trạm bên trong có thể truy cập tới bất kỳ SMTP server nào
- Cho phép các xác nhận từ SMTP server bên ngoài.

action	src	port	dest	port	flags	comment
allow	**our hosts**	*	*	*		**outgoing calls**
allow	*	*	*	*	**ACK**	**replies to our calls**
allow	*	*	*	**>102**		**Traffic to**

- Xử lý các kết nối FTP
- Hai kết nối được sử dụng: Một dùng để điều khiển và 1
- để truyền dữ liệu; dùng 2 cổng khác nhau (20, 21)
- Các kết nối ra ngoài sử dụng các cổng chỉ số cao (> 1023)

- *Ưu điểm:* đơn giản, nhanh, trong suốt với người dùng.
- *Nhược điểm:* rất khó để thiết lập các luật chính xác và không có khả năng chứng thực.

2) Các biện pháp thường được sử dụng để tấn công packet-filtering firewall: IP Spoofing, Source routing attack, Tiny fragment attack.

- IP address spoofing – các gói tin từ bên ngoài có sử dụng địa chỉ IP giả (tin cậy) trong trường địa chỉ nguồn.
- Source routing attacks – hacker ấn định tuyến nguồn để gói tin tránh các điểm kiểm soát.
- Tiny fragment attack – hacker phân nhỏ gói tin để qua mặt các luật lọc gói tin dựa trên tiêu đề TCP.

3)Stateless và Stateful firewall. Ưu điểm của Stateful firewall so với Stateless firewall.

- Stateless firewall: Các packet-filter firewall thông thường (tĩnh – static) là dạng stateless.
  - Lọc các gói tin độc lập, không tham chiếu các thông tin khác.
  - Nếu có một phân đoạn TCP SYN/ACK được gửi, không thể biết được trước đó đã có phân đoạn SYN để yêu cầu mở kết nối hay chưa (các stateful firewall có thể kiểm tra được).
  - Các stateless firewall không xử lý được các ứng dụng đảo cổng (e.g FTP):
    - FTP sử dụng cổng 21 để trao đổi thông tin điều khiển
    - Sử dụng cổng 20 để trao đổi dữ liệu.

- Stateful firewall:
    - Trạng thái của 1 kết nối: Open or Closed
        - State: Thứ tự của gói tin trong cuộc trao đổi
        - Thường cho biết gói tin có phải thuộc về một kết nối đang mở hay không.
    - Stateful Firewall Operation
        - Với TCP, ghi lại 2 địa chỉ và số hiệu cổng vào bảng trạng thái với tình trạng OK (mở)
            - Mặc định, cho phép các kết nối từ các trạm trong mạng tới các máy chủ ngoài mạng.
            - Các gói tin trao đổi tiếp theo giữa các máy này tại các cổng này là được phép mà không cần phải xem xét kỹ.
            - Bản ghi bị xóa khỏi bảng trạng thái khi kết nối TCP ngắt.
        - Với UDP, tương tự như TCP, 2 địa chỉ IP và số hiệu cổng được ghi lại trong bảng trạng thái với tình trạng OK
            - Bản ghi bị xóa khi xảy ra time-out
- Ưu điểm của Stateful firewall với Stateless firewall:
    - Stateful firewall có thể hiểu được trạng thái của gói tin (gói tin có thuộc về 1 kết nối đang mở hay không), stateless thì không
    - Stateless firewall không xử lý được ứng dụng đảo cổng