Phần 1: Câu hỏi lý thuyết

1. **Trình bày các hình thức tấn công? Nêu ví dụ minh họa? Liên hệ với các mục tiêu của an ninh mạng**

Trả lời:

* Các hình thức tấn công phổ biến và ví dụ minh họa:

+ Tấn công mạng với hình thức Phishing:

Người dùng rất dễ bị lừa nếu không để ý tới trang web mà mình đang truy cập bởi vì Phishing là kiểu tấn công người dùng bằng cách tạo ra 1 trang web với địa chỉ giả mạo. Chẳng hạn như www.google.com thành www.gugle.com. Thông thường với hình thức này, các tin tặc sẽ gửi tới người dùng 1 email đăng nhập để người dùng đăng nhập và click vào đó, tiếp theo sẽ sử dụng kỹ thuật điều hướng để điều sang website chứa mã độc. Và vô tình, khi bạn đăng nhập thông tin tài khoản gmail của mình vào web giả mạo đó, bạn đã bị mất tài khoản.

+ Tấn công mạng trực tiếp từ bên trong nội bộ

Tin tặc có thể cài gắm máy tính trực tiếp của họ vào máy tính của người khác hoặc lấy được tài khoản và mật khẩu của người khác sau đó thực hiện hành vi tấn công của mình

+ Tấn công gián tiếp

Các hacker có thể nghe trộm những thông tin khi truy cập vào hệ thống máy tính người dùng để đánh cắp dữ liệu cá nhân như hình ảnh, file, video…

+ Tấn công theo tệp đính kèm

Ví dụ như Email, file đính kèm chẳng hạn. Sau khi người dùng click vào tệp đính kèm thì lập tức máy tính bị nhiễm virus Hoặc mã độc tống tiền Ransomware có thể ẩn trong quảng cáo Skype, phần mềm trên điện thoại iPhone, Android.

+ Tấn công ẩn danh

Virus có thể xâm nhập vào máy tính bằng những phần mềm độc hại như những phần mềm diệt virus, phần mềm học tập hay các trình duyệt, plug in ẩn danh, ẩn trong quảng cáo của trình duyệt & phần mềm

+ Tấn công vào con người

Kẻ tấn công có thể liên lạc với người quản trị hệ thống, tạo nên 1 hộp thoại đăng nhập sau đó yêu cầu người dùng thay đổi mật khẩu, thay đổi cấu hình hệ thống. Phương tức tấn công mạng này rất khó tìm ra giải pháp ngăn chặn triệt để ngoài giáo dục nhận thức của người dùng.

+ Một số hình thức, phương thức tấn công vào hệ thống mạng, máy tính khác như: thông qua usb, đĩa CD, địa chỉ IP, server, qua đầu vào của máy in….

1. **Trình bày các mục tiêu của an ninh mạng? Lấy ví dụ?**

Trả lời:

Các mục tiêu của an ninh mạng là:

1. Bảo mật

VD: Một ví dụ về sự vi phạm bí mật:

Ai đó đọc các gói tin bản rõ được trao đổi giữa A và B bằng cách chạy một chương trình như Wireshark.

Nếu các gói tin được mã hóa an toàn mặc dù chúng bị người khác lấy đc, thì họ không thể đọc.

1. Toàn vẹn

VD: A và B không muốn những thông điệp của họ thay đổi bởi người khác. Đây là mục tiêu an ninh mạng của tính toàn vẹn.

1. Tính sẵn sàng

VD:

1. Tính xác thực người gửi và người nhận

VD:

1. Xác thực nguồn gốc thông tin

VD:

1. Đảm bảo việc xác thực không phụ thuộc vào nội dung cuộc nói chuyện

VD:

1. Tính không từ chối ở phía nguồn

VD:

1. Tính không từ chối ở phía đích

VD:

1. Tính xác thực

VD:

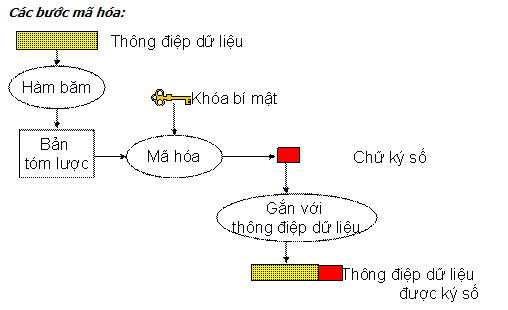
1. Điều khiển truy cập

VD:

1. **Khái niệm mã hóa công khai? Sử dụng mã hóa công khai làm chữ ký số?**

Trả lời:

* Mã hóa công khai công khai là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa bí mật.
* Mô hình Mã hóa khóa công khai tạo chữ kí số :



1. **Trình bày khái niệm firewall, cơ chế kiểm soát, ưu điểm và hạn chế?**

Trả lời:

* Firewall hay còn gọi là tường lửa được xem như một bức rào chắn giữa máy tính (hoặc mạng cục bộ - local network) và một mạng khác (như Internet), điều khiển lưu lượng truy cập dữ liệu vào ra. Nếu không có tường lửa, các luồng dữ liệu có thể ra vào mà không chịu bất kì sự cản trở nào. Còn với tường lửa được kích hoạt, việc dữ liệu có thể ra vào hay không sẽ do các thiết lập trên tường lửa quy đinh.
* Cơ chế kiểm soát:
* Kiểm soát dịch vụ: Xác định các loại dịch vụ Internet có thể được truy cập, gửi đi hoặc gửi đi
* Điều khiển hướng: Xác định hướng chỉ rõ các yêu cầu dịch vụ cụ thể
* Kiểm soát người dùng: Kiểm soát quyền truy cập vào một dịch vụ theo đó người dùng đang cố gắng truy cập nó
* Kiểm soát hành vi: Kiểm soát cách sử dụng các dịch vụ cụ thể (ví dụ: lọc e-mail)
* Ưu điểm và hạn chế

+ Ưu điểm:

* Đơn giản
* Chạy với tốc độ cao
* Các tính năng khác:

Dịch địa chỉ mạng (NAT)

Trạm chế độ ngầm IPSec (chế độ vận chuyển khác)

+ Hạn chế:

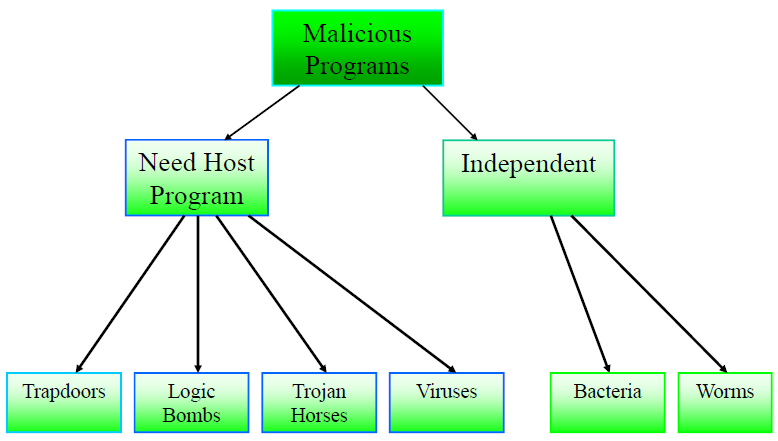
* Không thể bảo vệ chống lại các cuộc tấn công vượt qua tường lửa ví dụ: quay số trong modem trên LAN nội bộ
* Không thể bảo vệ chống lại các cuộc tấn công nội bộ ví dụ: một nhân viên không hài lòng.
* Không thể bảo vệ chống lại việc truyền virut. Trong hầu hết các trường hợp, hoặc là không thực tế hoặc không thể quét tất cả các dữ liệu và các tập tin được chuyển.

1. **Khái niệm về các phần mềm độc hại, phân loại?**

Trả lời:

* Phần mềm độc hại là phần mềm không mong muốn được cài đặt trên hệ thống của người dùng mà không được sự cho phép của họ.
* Phân loại phần mềm độc hại:

Có 2 loại phần mềm độc hại:



+ Khi lưu trữ chương trình :

* Trapdoor:cái Bẫy
* Logic Bombs
* Trojan horses
* Viuses

+ Phần mềm độc hại độc lập:

* Bacteria:vi khuẩn
* Worms:sâu

1. **Phân loại firewall? Trình bày về cơ chế Package Filtering?**

Trả lời:

* Phân loại tường lửa:

Có 3 loại tường lửa thông dụng:

* Packet‐filtering firewall
* Circuit‐level gateway
* Application‐level gateway
* Trình bày về cơ chế Packet-filtering:

Packet-filtering thường được thiết lập bởi một tệp tin cấu hình. Tập lệnh cho phép hạn chế quyền truy cập.

Packet-filtering Thường lọc các gói theo các tiêu chí sau: Tiêu chí thường có thể kết hợp với nhau qua:

* Địa chỉ IP của nguồn hoặc đích
* Cảng Số lượng hoặc đích
* Giao diện phần cứng
* Packet Type-tcp, udp, icmp
* Các đặc tính gói tin

1. ***Khái niệm về các phần mềm độc hại, phân loại?***
2. ***Nêu các hình thức tấn công? Liên hệ với các mục tiêu của an ninh mạng***
3. **Trình bày về Circuit‐level Gateway trong firewall?**

Trả lời:

Circuit-level Gateway: Hoạt động tại lớp session của mô hình OSI, nó giám sát các gói tin “handshaking” đi qua firewall, gói tin được chỉnh sửa sao cho nó xuất phát từ circuit-level Gateway.Khi thực thi nó giúp che dấu thông tin cá nhân trong mạng cần được bảo vệ.

1. **Trình bày về các loại firewall topology?**

Có 3 loại firewall topology là:

-Perimeter : đây là mô hình firewall phổ biến nhất ,mô hình gồm 1 firewall đặt nằm giữa các vùng mạng hoặc giữa các hệ thống tin cậy và không tin cậy.

-Three-Legged (DMZ) : mô hình này thường được sử dụng khi chúng ta muốn tài nguyên ra các hệ thống mạng bên ngoài , khu vực mạng chứa các tài nguyên này được gọi là DMZ. Cũng giống như mô hình Perimeter , mô hình này sử dụng 1 tường lửa nhưng có thêm 1 card mạng khác kết nối với DMZ. Tường lửa sẽ được cấu hình cho phép bên ngoài truy cập đến những tài nguyên được chỉ định.

- Chained (DMZ) : mô hình này sử dụng 2 tưởng lửa để tạo DMZ nằm ở giưa hệ thống mạng nội bộ và bên ngoài. Việc cấu hình cho 2 firewal này tưởng đổi phức tạp , nhưng nếu cấu hình đúng thì mô hình tường lủa này mang lại hiệu quả rất cao. Mô hình này thường được áp dụng khi mạng nội bộ và mạng bên ngoài muốn truy cập vào DMZ, sẽ có các rule ở mỗi tường lửa cho từng truy cập từ bên ngoài và bên trong

**11.Khái niệm chữ ký số? Sử dụng mã hóa công khai thực hiện giao dịch có chữ ký số?**

"Chữ ký số" là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác

Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa;

Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

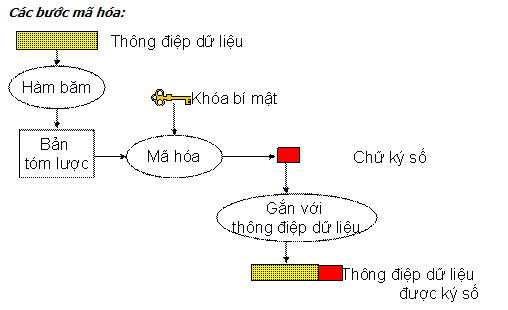
“Hệ thống mật mã không đối xứng” là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá bí mật và khoá công khai.

“Khoá” là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.

“Khóa bí mật” là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.

“Khóa công khai” là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khoá bí mật tương ứng trong cặp khoá

**Sử dụng mã hóa công khai thực hiện giao dịch có chữ ký số?**



**12.Trình bày các bước để mã hóa theo thuật toán Ceasar Cipher? Lấy ví dụ mã hóa một chuỗi ký tự tùy chọn để minh họa**

 Bước 1: Đưa tất cả 26 chữ cái Tiếng Anh vào trong một vòng tròn.

- Bước 2: Khởi tạo giá trị cho**K** (K - số lần dịch chuyển)

- Bước 3: Để mã hóa một chữ cái thì ta dịch chuyển nó K đơn vị theo chiều kim đồng hồ.

- Bước 4: Sau khi mã hóa, ta thu về được một đoạn chuỗi là chuỗi mã hóa của chuỗi ban đầu.

Ví dụ minh hoạ.

Với k = 3  
Chuỗi ban đầu ta có: **AN NINH MẠNG**

Ta dịch A sang 3 đơn vị thành D

N 3 Q

I 3 L

H 3 K

M 3 P

G 3 J  
Chuỗi sau khi mã hóa: **DQQLQKPDQJ**

**Giải mã**

Bước 1: Đưa tất cả 26 chữ cái Tiếng Anh vào trong một vòng tròn.

Bước 2: Xác định số**K,**thường là đã biết trước

Bước 3: Để giải mã một chữ cái thì ta dịch chuyển nó K đơn vị ngược chiều kim đồng hồ.

Bước 4: Sau khi giải mã, ta thu về được một đoạn chuỗi là chuỗi giải mã của chuỗi ban đầu.

**13.Khi trao đổi thông điệp qua mạng tính toàn vẹn (integrity) được yêu cầu thế nào? Thực hiện yêu cầu toàn vẹn bằng giải pháp nào?**

Yêu cầu tính toàn vẹn  là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

Đúng, Chính xác, Không bị thay đổi, thay đổi nhưng phải theo cách chấp nhận được, Chỉ người được phép thay đổi được, Chỉ quá trình xử lí hợp thức mới thay đổi dc, Nhất quán,Nhất quán nội tại, Các kết quả đúng và có ý nghĩa

Giải pháp : …………………………………….

**14.Trình bày các bước để mã hóa theo thuật toán Vigenere Cipher? Lấy ví dụ mã hóa một chuỗi ký tự tùy chọn để minh họa.**

B1: viết bản rõ ra

B2. Viết từ khoá lặp nhiều lần phía trên tương ứng của nó

B3 : sử dụng mỗi chữ của từ khoá như khoá của mã Ceasar. Mã tương ứng của bản rõ với bước nhảy tương ứng

(Ta tìm ký tự mà là giao của của cột ký tự khoá và hàng ký tự bản rõ.)

VD : key lemon

B1 Bản rõ  **A T T A C K A T D A W N**

B2 L E M O N L E M O N L E M

Chữ cái đầu tiên của văn bản, A, được mã hóa bằng bảng bắt đầu với L (chữ cái đầu tiên của từ khóa). Nó sẽ được mã hóa thành chữ cái trên dòng L và cột A của hình vuông Vigenère, đó là chữ L. Tương tự như vậy, chữ cái thư hai của văn bản sẽ được mã hóa bằng chữ cái thứ hai của từ khóa: chữ trên dòng E và cột T là X

Ta được bản mã LXFOPVEFRNHR

**15.Nêu các hạn chế của firewall? Các cơ chế thiết lập firewall?**

\*Hạn chế của firewall

- Không thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nếu không được xác định rõ các thông số địa chỉ.

- không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không đi qua nó.

- không thể chống lại các cuộc tấn công bằng dữ liệu

- không thể làm nhiệm vụ và quét virut trên các dữ liệu khi được truyền qua nó

- có thể làm chậm kết nối khi xử lí các thông tin

-Chỉ hữu hiệu đối với những người không thành thạo kĩ thuật vượt firewall

\*Cơ chế thiết lập firewall

Firewall hoạt động chặt chẽ với giap thức TCP/IP , vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức(Telnet, SMTP,DNS,SMNP,NFS..) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan đến rất nhiều các packet và những con số địa chỉ của chúng , bộ lọc packet cho phép hay từ chôi mỗi packet mà nó nhận được, Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoã mãn một trong số các luật lệ của lọc packet hay không.Các luật lệ lọc packet này dựa trên các thông tin ở đầu mỗi packet, dung để cho phép truyền các packet đó ở trên mang. Bao gồm:

Địa chỉ IP nơi xuất phát (Source)

Địa chỉ IP nơi nhận (Destination)

Những thủ tục truyền tin (TCP,UDP,ICMP,IP tunnel..)

Cổng TCP/UDP nơi xuất phát

Cổng TCP/UDP nơi nhận

Dạng thông báo ICMP

Giao diện packet đến

Giao diện packet đi

Nếu packet thoả các luật lệ đã được thiết lập trước của fire wall thì packet đó được chuyển qua, nếu không thoả sẽ bị loại bỏ. Việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định được phép mưới vào được hệ thống mạng cục bộ.Nên cũng lưu ý là do việc kiểm tra dựa trên header của các packet nên bọ 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. Trong các phần sau chúng ta sẽ tìm hiểu các kỹ thuật để vượt tường lửa.

1. **Trình bày cách thiết lập một bộ khóa trong thuật toán RSA. Sử dụng bộ khóa đó để mã hóa và giải mã một ký tự tùy chọn**

\* khóa của RSA được sinh như sau:

* Chọn 2 số nguyên tố p và q
* Tính n = pq. Sau này, n sẽ được dùng làm modulus trong cả public key và private key.
* Tính một số giả nguyên tố bằng [phi hàm Carmichael](http://math-it.org/Mathematik/Zahlentheorie/Carmichael.html) như sau: λ(n) = BCNN(λ(p), λ(q)) = BCNN(p − 1, q − 1). Giá trị này sẽ  
  được giữ bí mật.
* Chọn một số tự nhiên e trong khoảng (1, λ(n)) sao cho ƯCLN(e, λ(n)) = 1, tức là e và λ(n) nguyên tố cùng nhau.
* Tính toán số d sao cho d ≡ 1/e (mod λ(n)) hay viết dễ hiểu hơn thì de ≡ 1 (mod λ(n)). Số d được gọi là số nghịch đảo modulo của e (theo modulo mod λ(n)).

Public key sẽ là bộ số (n, e), và private key sẽ là bộ số (n, d). Chúng ta cần giữ private key thật cẩn thận cũng như các số nguyên tố p và q vì từ đó có thể tính toán các khóa rất dễ dàng.

Trong thực hành, chúng ta thường chọn e tương đối nhỏ để việc mã hóa và giải mã nhanh chóng hơn. Giá trị thường được sử dụng là e = 65537. Ngoài ra, chúng ta có thể tính số giả nguyên tố bằng [phi hàm Euler](http://math-it.org/Mathematik/Zahlentheorie/Euler.html) φ(n) = (p − 1)(q − 1) và dùng nó như λ(n). Vì φ(n) là bội của λ(n) nên các số d thỏa mãn de ≡ 1 (mod φ(n)) cũng sẽ thỏa mãn d ≡ 1/e (mod λ(n)). Tuy nhiên, một số tác dụng phụ của việc này là d thường sẽ trở nên lớn hơn mức cần thiết.

**Sử dụng bộ khóa đó để mã hóa và giải mã một ký tự tùy chọn**

**(**bài tập hôm trước mấy đứa làm trên lớp. các ông mở ra xem nhé, t ngại gõ lại :v)

**17.Nêu những hiểu biết của bạn về hàm băm (Hash function) và sử dụng hàm băm trong đảm bảo tính toàn vẹn của thông điệp?**

**Hàm băm** là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán ***h*** một chiều nào đó, rồi đưa ra một bản băm – văn bản đại diện – có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.

**Đặc trưng:**

Hàm băm *h* là hàm một chiều (one-way hash) với các đặc tính:

Với thông điệp đầu vào *x* thu được bản băm ***z* = *h*(*x*)** là duy nhất.

Nếu dữ liệu trong thông điệp *x* thay đổi để thành thông điệp *x*’ thì ***h*(*x*’) ≠ *h*(*x*)** => Hai thông điệp hoàn toàn khác nhau thì giá trị hàm băm cũng khác nhau.

Nội dung của thông điệp gốc không thể bị suy ra từ giá trị hàm băm => Với thông điệp *x* thì dễ dàng tính được *z* = *h*(*x*), nhưng lại không thể (thực chất là khó) suy ngược lại được *x* nếu chỉ biết giá trị hàm băm *h*

**Vai trò** hàm băm trong mật mã hiện đại:

Được dùng để xác thực tính nguyên vẹn dữ liệu

Được dùng trong quá trình tạo chữ kí số trong giao dịch điện tử.

Các hàm băm lấy một thông báo đầu vào và tạo một đầu ra được xem như là:

Mã băm (hash code),

Kết quả băm (hash result),

Hoặc giá trị băm (hash value).

**sử dụng hàm băm trong đảm bảo tính toàn vẹn của thông điệp?**

Giải pháp cho các vấn đề vướng mắc đến chữ ký số là dùng “**hàm băm”** để trợ giúp cho việc ký số

Các thuật toán băm với đầu vào là các bức thông điệp có dung lượng, kích thước tùy ý (vài KB đến vài chục MB …) – các bức thông điệp có thể là dạng văn bản, hình ảnh, âm thanh, file ứng dụng v.v… - và với các thuật toán băm: MD2, MD4, MD5, SHA cho các bản băm đầu ra có kích thước cố định: 128 bit với dòng MD, 160 bit với SHA1.

Như vậy, bức thông điệp kích thước tùy ý sau khi băm sẽ được thu gọn thành những bản băm – được gọi là các “**văn bản đại diện”** – có kích thước cố định (128 bit hoặc 160 bit).

Với mỗi thông điệp đầu vào chỉ có thể tính ra được một văn bản đại diện – giá trị băm tương ứng – duy nhất

Hai thông điệp khác nhau chắc chắn có hai văn bản đại diện khác nhau. Khi đã có văn bản đại diện duy nhất cho bức thông điệp, áp dụng các sơ đồ chữ ký số ký trên văn bản đại diện đó

**18.Nêu kiến trúc các mô hình cài đặt firewall?**

**-Thứ nhất : Kiến trúc Dual-homed Host**

Được xây dựng dựa trên máy tính dual-home host. Một máy tính được gọi là dual-homed host nếu có ít nhất 2 network interface, có nghĩa là máy đó có gắn 2 card giao tiếp với 2 mạng khác nhau , do đó máy tính này đóng vai trò là router mềm, Kiến trúc dual-home host rất đơn giản, máy dual-home host ở giữa, một bên được nối với internet và bên còn lại nối với mạng nội bộ.

Gồm có các đặc điểm sau:

-phải disable chức năng routing của dual-homed host để cấm hoàn toàn thông IP từ ngoài vào

Các hệ thống bên ngoài và bên trong dual-home host mà chúng không liên lạc trực tiếp được với nhau.

Dual homed host cung cấp dịch vụ thông qua poxy server hoặc login trực tiếp vào dual –home host.

-**Thứ hai : Kiến trúc Screened Host**

Trong kiến trúc này chức năng bảo mật chính được cung cấp bởi chức năng packet filtering tại screening router.

Packet filtering trên screening router được setup sao cho basition host là máy duy nhất trong internal network mà các host trên internet có thể mở kết nối đến Packet filtering cũng cho phép bastion host mở các kết nối ra bên ngoài.

Các packet filtering thực hiện công việc sau:

Cho phép các interal hosts mở kết nối đến các host trên internet đối với một số dịch vụ được phép

Cấm tất cả kết nối từ các interal hosts

**-Thứ ba : Kiến trúc Screened Subnet Host**

Thêm một perimeter network để cô lập interal network với internet.Như vật dù hacker đã tấn công được vào bastion host vẫn còn một rào chắn nữa phải vượt qua interior router. Các lưu thông trong internet network được bảo vệ an toàn cho dù bastion đã bị “ chiếm”. Các dịch vụ nào ít tin cậy và có khả năng dễ bị tấn công thì nên để ở perimeter network.Bastion host là điệm liên lạc cho các kết nối từ ngoài vào :SMTP, FTP,DNS . Còn đối với viêc truy cập các dịch vụ từ internal client đến các server trên internet thì được điều khiển như sau:

Setup packet filtering trên các exterior và interior router để cho phép internal client truy cập các servers bên ngoài 1 cách trực tiếp.

Setup poxy server tren bastion host để cho phép internal clients truy cập các server bên ngoài 1 cách gián tiếp.