**Tóm gọn :** cuối kỳ lý thuyết nhiều ko có các câu tính nào cả ( đem máy tính cũng ko dùng đến , mà cứ đem cho có :v có khi năm nay thầy cho các câu tính của RSA thì sao :v ) . Nội dung thường nằm trong SLIDE mà ko ở mức chi tiết lắm chỉ ở mức hiểu thôi .

1)Dùng Cesar mã hóa:”I must pass this exam”->..

2)A dùng khóa đối xứng muốn gửi thông điệp có chữ ký số cho B.B cần gì để đọc:

3)A dùng khóa bất đối xứng muốn gửi thông điệp cho B.B cần gì để đọc:

Câu 2 3 có đáp án như nhau :public key A-public key B-private key A-private B

4)loại nào nhân bản trong máy :

5)Loại nào không nhân bản khi chạy 1 ứng dụng có lợi:

Câu 4 5: worn-virus-**trojan**-logic bomb

6)Kiểu tấn công sử dụng lỗ hổng SQL : SQLcracking-**SQL injection**-… ( trong đề thi 2016 thì thầy ko cho SQL Injection vào , mà có câu D là các đáp án đều sai )

7)Thế nào là vi phạm tính bảo mật trong 1 công ty: Nhân viên dùng thông tin vào mục đích cá nhân-…

8)Kiểu tấn công chỉ nghe ngóng thông tin để bắt được 1 cái gì đó :Pass,account,… thuộc nhóm:DoS-man in the middle….

9)Kiểu tấn công dùng từ điển của hacker thuộc nhóm nào: DoS-hacking-…

10)Buffer overload là kiểu tấn công:

-Làm tràn buffer

-Làm tràn bộ nhớ đệm

-Làm vượt quá khả năng tính toán cho các biến ….

11)RSA dùng để mã hóa thông điệp có kích thước : 32bit-64bit-32byte-64byte

12)Mã băm là mã gì? -> Có các block vào kích thước có thể k0 giống nhau nhg block ra thì giống nhau

13) Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là:-CBC- ECB -CFB - OFB14) Bức tường lửa dùng để?. …

15) Cơ chế bảo mật SSL hoạt động trên tầng-.Network, Transport -Network, Session -Application, Session

16)Chữ kí điện tử dùng để ?….

17)Sử dụng tên người dùng giả là kiểu tấn công gì ? -sniffing-…

18)Zombie máy tính là gì? -> Liên quan đến cuộc tấn công DDOS ấy , hình như nó là các máy con bị điều khiển để cùng mục đích tấn công vào một nạn nhân nào đó …

19)Chữ ký thuộc kiểu nào trong các kiểu xác định người dùng?-người dùng có-người dùng biết-sinh trắc học-…

20) SSL with HTTPS sử dụng cổng nào? -TCP80-TCP443-UDP8080-…

21) Dùng Rail Fence mã hóa chuỗi …. ( Cái này thuộc hoán vị dễ ồm -> nên coi lại )

**BẢN DỊCH CHƯƠNG 11**

mã di động nói đến các chương trình (ví dụ, script macro, hoặc hướng dẫn cầm tay khác) có thể được vận chuyển giữ nguyên cho một bộ sưu tập không đồng nhất của các nền tảng và thực hiện với ngữ nghĩa giống nhau

mã di động được truyền từ một hệ thống từ xa đến một hệ thống địa phương và sau đó thực hiện trên hệ thống địa phương mà không cần hướng dẫn rõ ràng của người dùng

mã di động thường hoạt động như một cơ chế cho một loại virus, sâu, hoặc Trojan horse được truyền đến máy trạm của người dùng

Trong trường hợp khác, mã di động lợi dụng lỗ hổng để thực hiện khai thác riêng của mình, chẳng hạn như truy cập dữ liệu trái phép hay thỏa hiệp gốc

**Multiple-Threat Malware**

* virus và phần mềm độc hại khác có thể hoạt động trong nhiều cách khác nhau.
* Một virus lây nhiễm chia ra nhiều phần trong nhiều cách
* Thông thường, **multipartite virus chia ra nhiều phần** có khả năng lây nhiễm cho nhiều loại tập tin, do đó tiêu diệt virus phải đối phó với tất cả các site có thể bị nhiễm trùng
* **Một cuộc tấn công hỗn hợp** sử **dụng nhiều phương pháp** lây nhiễm hoặc truyền dẫn, để tối đa hóa tốc độ lây lan và mức độ nghiêm trọng của vụ tấn công.
* Một ví dụ về một cuộc tấn công hỗn hợp là cuộc tấn công Nimda **Nimda attack**, hay bị gọi nhầm là chỉ đơn giản là một con sâu.
* Nimda sử dụng bốn phương pháp phân phối:
  + E-mail:
  + Windows shares:
  + Web servers:
  + Web clients:

**Viruses**

* mảnh phần mềm mà lây nhiễm các chương trình
* Sửa đổi chúng để **tạo một bản sao của virus**
* để nó thực hiện bí mật khi **chương trình chủ** được chạy.
* Xác định cho hệ điều hành và phần cứng

• lợi dụng chi tiết và yếu điểm của chúng

**Virus structure**

**A computer virus has three parts:**

**Cơ chế lây nhiễm (Infection mechanism)** : Các phương tiện mà một loại virus lây lan, cho phép nó để nhân rộng. Cơ chế này cũng được gọi là vector lây nhiễm.

**Trigger :** Các sự kiện hoặc điều kiện xác định khi tải trọng được kích hoạt hoặc chuyển giao.

**Payload :** Điều gì virus làm, bên cạnh lan rộng. Payload có thể gây tổn thương hoặc có thể liên quan đến hoạt động lành tính nhưng đáng chú ý.

**Giai đoạn Virus**

Một virus thông thường đi qua bốn giai đoạn sau đây:

**Giai đoạn không hoạt động** - **nằm ngủ** ( **Dormant phase) : Virus là nhàn rỗi**. Vi rút cuối cùng sẽ được kích hoạt bởi một số sự kiện, chẳng hạn như một ngày, sự hiện diện của một chương trình khác hoặc tập tin, hoặc dung lượng của đĩa vượt quá giới hạn một số. Không phải tất cả các virus có giai đoạn này.

**Giai đoạn lan truyền ( Propagation phase ) :** Virus đặt một bản sao của chính nó vào các chương trình khác hoặc vào các khu vực hệ thống nhất định trên đĩa. **Bản sao có thể không giống với phiên bản nhân giống**; virus thường biến hình để tránh bị phát hiện. Mỗi chương trình bị nhiễm bây giờ sẽ có một bản sao của virus, mà bản thân nó sẽ bước vào một giai đoạn tuyên truyền.

**Giai đoạn kích hoạt (Triggering phase):** **Virus được kích hoạt** để thực hiện các chức năng mà nó được dự định. Cũng như với các giai đoạn không hoạt động, giai đoạn kích hoạt có thể được gây ra bởi một loạt các sự kiện hệ thống, bao gồm cả một số của số lần mà bản sao của virus đã làm bản sao của chính nó

**Giai đoạn thực thi (Execution phase):** Các chức năng được thực hiện. Các chức năng có thể là vô hại, chẳng hạn như một tin nhắn trên màn hình, hoặc gây tổn hại, chẳng hạn như sự phá hủy của các chương trình và các tập tin dữ liệu

**Phân loại Virus**

1.Một phân loại vi rút ***theo từng mục******tiêu******( by target )*** bao gồm các danh mục sau :

* **Boot sector lây nhiễm**: lây nhiễm một **record boot master** hoặc **boot record** và lây lan khi một hệ thống được khởi động từ ổ đĩa USB chứa virus.
* **Lây nhiễm tâp tin ( File )** : lây nhiễm các tập tin mà hệ điều hành ( **the operating system )** hoặc **shell** xem xét là thực thi.
* **Virus macro:** lây nhiễm các tập tin với mã vĩ mô **(macro code)** được thể hiện bởi một ứng dụng.

2.Một phân loại virus **bằng chiến lược che giấu *(concealment strategy)***bao gồm các danh mục sau:

**Virus mã hóa (Encrypted virus*):*** *Một phần của virus tạo một khóa mã hóa ngẫu nhiên và mã hóa phần còn lại của virus*. Các khóa được lưu trữ với virus. Khi một chương trình bị nhiễm được gọi, virus sử dụng chìa khóa ngẫu nhiên được lưu trữ để giải mã virus. Khi virus nhân lên, một chìa khóa khác nhau ngẫu nhiên được chọn.Bởi vì phần lớn các virus được mã hóa với một khóa khác nhau cho mỗi trường hợp, không có chút mô hình liên tục để quan sát.

**Virus tàng hình ( virus stealth ):** Một dạng virus được thiết kế một cách rõ ràng **để tự ẩn từ sự phát hiện của các phần mềm chống virus** **(hide itself from detection).** Như vậy, toàn bộ virus, không chỉ là một tải trọng là ẩn.

**Virus đa hình** **( Polymorphic virus ) :** Là một loại virus đột biến với tất cả các nhiễm trùng , làm cho sự phát hiện của các "chữ ký" **( signature )** liên quan đến không thể đạt đc virus.

**Virus siêu đa hình ( Metamorphic virus)** : **Là một loại virus đa hình**, một đột biến từ virus siêu đa hình với tất cả các nhiễm trùng. Sự khác biệt là một loại virus siêu đa hình **có thể viết lại bản thân hoàn toàn tại mỗi lần lặp** , tăng khó khăn trong việc phát hiện.

**Macro virus** : giữa những năm 1990 -> phổ biến ->lây nhiễm sang các tài liệu ( Mirosoft Word hoặc Microsoft office ) ko phải là chương trình máy tính -> dễ lây lan ( qua thư điện tử - email ) -> khó kiểm soát nếu chỉ kiểm soát các truy cập hệ thống.

**Email virus** : -> phát triển gần đây , vd : **Melissa , đc đính kèm trong tập tin MS Word -> nếu người nhận mở file đính kèm e-mail , -> người dùng mở tệp đính kèm -> virus kích hoạt ->**

* Các virus e-mail tự gửi đến tất cả mọi người trong danh sách gửi thư trong gói e-mail của người dùng.
* Vi rút gây sát thương cục bộ trên hệ thống của người dùng.

**Biện pháp đối phó Virus**

- **Phòng chống** - giải pháp lý tưởng nhưng khó khăn

- Thực tế cần:

* + **nhận diện (detection)**
  + **nhận biết (identification)**
  + **gỡ bỏ (removal)**

- Nếu phát hiện nhưng không thể nhận biết (**identification)** hoặc loại bỏ (**removal)** , thì giải pháp thay thế là **hủy bỏ (discard)** các tập tin bị nhiễm và tải lại một phiên bản dự phòng sạch.

**Sự Phát Triển (Evolution) Anti-Virus**

Những tiến bộ trong công nghệ chống virus và virus liên quan chặc chẽ với nhau . Virus ban đầu là những đoạn mã tương đối đơn giản và có thể được xác định và thanh lọc với các gói phần mềm chống virus tương đối đơn giản.

Như chạy đua vũ trang virus đã phát triển, cả virus và phần mềm chống virus đã trở nên phức tạp và tinh vi hơn.

Các thế hệ

* + Thế hệ đầu tiên: các máy quét đơn giản ( **Simple scanner** )
  + Thế hệ thứ hai: các máy quét heuristic ( **Heuristic scanners** )
  + Thế hệ thứ ba: các bẫy hoạt động ( **Activity traps** )
  + Thế hệ thứ tư: bảo vệ full-tính năng (**full-featured protection**)

**Kỹ Thuật Tiên Tiến Antivirus (Advanced Antivirus Techniques)**

**Giải mã tổng quát (Generic Decryption )**

* công nghệ cho phép các chương trình chống virus để **dễ dàng phát hiện** ngay cả những virus đa hình phức tạp nhất trong khi duy trì tốc độ quét nhanh

**Hệ thống miễn dịch kỹ thuật số ( Digital Immune System )** -> dùng đễ giám sát , phát hiện có phải virus không ?

**Phần mềm ngăn chặn-hành vi ( Behavior-blocking Software )** -> ngăn chặn các hành vi trc khi chúng đc thực hiên vd xóa sữa xem ……v…..

**WORMs**

- Một con sâu **là một chương trình** có thể tự tái tạo và gửi bản sao từ máy tính đến máy tính thông qua kết nối mạng.

- Khi đến nơi, sâu có thể được **kích hoạt** để tái tạo và lan truyền tiếp.

- Ngoài nhân giống, worm thường thực hiện một số chức năng không mong muốn.

- Một **virus e-mail** có một số đặc điểm của một con sâu bởi vì nó truyền bá từ hệ thống vào hệ thống.

- Tuy nhiên, chúng ta vẫn có thể phân loại nó như là **một virus**, vì nó sử dụng một tài liệu sửa đổi để chứa nội dung vĩ mô của virus và đòi hỏi hành động của con người.

- Một con sâu tích cực **tìm nhiều** máy móc hơn để lây nhiễm và mỗi máy đã bị nhiễm phục vụ như là một bệ phóng tự động cho các cuộc tấn công vào các máy khác

- Các chương trình worm network sử dụng kết nối mạng để lây lan từ hệ thống để hệ thống

- Khi **active** trong một hệ thống, một **con sâu mạng có thể hành xử như một virus máy tính hoặc vi khuẩn**, hoặc nó có thể cấy ghép các **chương trình Trojan horse** hoặc thực hiện bất kỳ số lượng các hành động gây rối hoặc phá hoại.

**Để tái tạo chính nó, một con sâu mạng sử dụng một số loại phương tiện mạng**

* **Cơ sở thư điện tử ( Electronic mail facility )** -> khi xem mail hoặc file đính kèm.
* **Khả năng thực hiện từ xa ( Remote execution capability )** -> thực hiện trên bản sao or lỗ hỏng chương trình dịch vụ mạng nào đó
* **Khả năng đăng nhập từ xa ( Remote login capability )** -> login vào hệ thống -> sau đó sao chép -> thực thi

**- Worm có các đặc điểm giống virus máy tính có 4 giai đoạn .**

- Những con sâu mạng cũng có thể cố gắng để xác định liệu một hệ thống trước đây đã bị nhiễm trước khi sao chép chính nó vào hệ thống.

- Trong một hệ thống multiprogramming, nó cũng có thể che giấu sự hiện diện của nó bằng **cách đặt tên chính nó như là một quá trình hệ thống hoặc sử dụng một số tên khác mà có thể không được nhận ra bởi một nhà điều hành hệ thống.**

- **Khi các virus, sâu mạng rất khó để chống**

**The Morris Worms**

một trong những tốt nhất biết sâu

 phát hành bởi **Robert Morris vào năm 1988**

 tấn công vào các hệ thống UNIX

• nứt tập tin mật khẩu để sử dụng tên đăng nhập / mật khẩu để

đăng nhập vào hệ thống khác

• khai thác một lỗi trong giao thức ngón tay

• khai thác một lỗi trong sendmail

 nếu thành công, có thể truy cập từ xa shell

• gửi chương trình bootstrap để sao chép sâu hơn

**Các cuộc tấn công Worm gần đây**

* **Code Red**
  + Tháng 7 năm 2001 khai thác MS IIS lỗi
  + thăm dò địa chỉ IP ngẫu nhiên, không tấn công DDoS
* **Code Red II biến thể bao gồm backdoor**
* **SQL Slammer**
  + Đầu năm 2003, tấn công MS SQL Server
* **Mydoom**
  + loạt gửi thư e-mail sâu xuất hiện vào năm 2004
  + cài đặt backdoor truy cập từ xa vào hệ thống bị nhiễm bệnh
* **Warezov family of worms**
  + scan for e-mail addresses, send in attachment

**Công nghệ Worm ( Worm Technology )**

DDOS

* send **ICMP ECHO packets**

Một cuộc tấn công từ chối dịch vụ (DoS) là một nỗ lực để ngăn chặn người sử dụng hợp pháp của một dịch vụ từ việc sử dụng dịch vụ đó.

Khi cuộc tấn công này xuất phát từ một máy chủ duy nhất hoặc nút mạng, sau đó nó được gọi đơn giản là một cuộc tấn công DoS.

Một mối đe dọa nghiêm trọng hơn được đặt ra bởi một cuộc tấn công DDoS.

Trong một cuộc tấn công DDoS, kẻ tấn công có thể tuyển dụng một số lượng host khắp Internet để đồng thời hoặc trong một thời trang phối hợp khởi động một cuộc tấn công vào các mục tiêu.

Phần này là có liên quan với các cuộc tấn công DDoS.

DDoS tấn công trực tiếp

• những kẻ tấn công có thể cấy phần mềm zombie trên một số trang web phân phối trên toàn mạng Internet.

• Thông thường, các cuộc tấn công DDoS liên quan đến hai cấp độ của máy tính zombie: zombie chủ và zombie nô lệ.

• Các máy chủ của cả hai máy đã bị nhiễm mã độc

Bước đầu tiên trong một cuộc tấn công DDoS là cho những kẻ tấn công để lây nhiễm một số máy với phần mềm zombie

 Các thành phần thiết yếu trong giai đoạn này của cuộc tấn công như sau:

1. Phần mềm có thể thực hiện các cuộc tấn công DDoS. Phần mềm này phải có khả năng chạy trên một số lượng lớn các máy móc, phải có khả năng che giấu sự tồn tại của nó, phải có khả năng giao tiếp với kẻ tấn công hoặc có một số loại cơ chế thời gian kích hoạt, và phải có khả năng khởi động các cuộc tấn công nhằm mục đích hướng tới mục tiêu.

2. Một lỗ hổng trong một số lượng lớn các hệ thống này. Những kẻ tấn công phải trở thành nhận thức của một lỗ hổng mà các quản trị hệ thống và người dùng cá nhân đã thất bại trong việc vá lỗi và cho phép kẻ tấn công để cài đặt các phần mềm zombie.

3. Một chiến lược định vị máy dễ bị tổn thương, một quá trình được gọi là quét

Nói chung, có ba dòng phòng thủ chống lại các cuộc tấn công DDoS: