Trac nghiem an ninh mang

03/04/2010 16:00
Đinh Xuân Dụy

1.Yêu cầu để đảm bảo sử dụng mã hóa đối xứng là
a.Có thuật tóan encryption tốt,có một khóa bí mật được biết bởi người nhận/gởi và kênh truyền bí mật để phân phát key
b.Có một kênh truyền phù hợp và một khóa bí mật được biết bởi người nhận/gởi
c.Có thuật tóan encryption tốt và có một khóa bí mật được biết bởi người nhận/gởi
d.Tất cả đều đúng
2.Các thuật tóan nào sau đây là thuật tóan mã hóa đối xứng
a.Triple –DES, RC4, RC5, Blowfish
b.Triple –DES, RC4, RC5, IDEA
c.RC4, RC5, IDEA, Blowfish
d.IDEA, Blowfish, AES, Elliptic Cure
3.Các phát biểu sau đây phát biểu nào đúng
a. Hầu hết các thuật tóan mã hóa đối xứng đều dựa trên cấu trúc thuật tóan Feistel
b.Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa
c.Hầu hết các thuật tóan mã hóa khối đều đối xứng
d.Tất cả đều đúng
4.Cơ chế bảo mật SSL hoạt động trên tầng
a.Network, Transport
b.Network, Session
c.Application, Session
d.Tất cả đều sai
5.Keberos là dịch vụ ủy thác
a. Xác thực trên Web
b. Xác thực X.509
c. Xác thực trên Server
d. Xác thực trên các máy trạm với nhau
6.PGP là giao thức để xác thực
a. Quyền đăng cập vào hệ thống máy chủ Window
b. Bảo mật cho thư điện tử
c. Thực hiện mã hóa thông điệp theo thuật tóan RSA
d. Địa chỉ của máy trạm khi kết nối vào Internet
7. Công cụ/cơ chế bảo mật cho mạng không dây là
a. SSL
b. TSL
c. Giao thức PGP
d. WEP
8. Giao thứ SSL và TSL hoạt động ở tầng nào của mô hình OSI
a. Network
b. Sesion

c. Transport
d. **Từ tầng Trasport trở lên**
9. Giao thức SSL dùng để
a. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP
b. Cung cấp bảo mật cho thư điện tử
c. **Cung cấp bảo mật cho Web**
d. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window
10.Chức năng chính của Virus là
a. Lây nhiễm và sinh sản
b. Sống ký sinh và lây nhiễm
c. Tự phát triển độc lập và lây nhiễm
d. Tất cả đều đúng
11.Hoạt động của virus có 4 giai đoạn
a. Nằm im, lây nhiễm, tàn phá và tự hủy
b. Lây nhiễm, tấn công, hủy diệt và tự hủy
c. Nằm im, lây nhiễm, khởi sự và tàn phá
d. Lây nhiễm, khởi sự, tàn phát, kích hoạt lại
12.Các dạng sau đây, dạng nào là của virus
a.sealth, cư trú bộ nhớ, macro, đa hình, file
b.stealth, cư trú bộ nhớ, macro, lưỡng tính, file
c.virus ký sinh, file, boot secctor, stealth, cư trú bộ nhớ, macro
d.virus ký sinh, cư trú bộ nhớ, boot secctor, Stealth, đa hình, macro
13. Virus Macro chỉ có khả năng tấn công vào các file
a. MS.Exel, MX Word, MS.Outlook Mail
b. MS.Exel, MX Word, MS.Power Point
c. MS.Exel, MX Word,Yahoo Mail
d.Tất cả các loại file
14. Các giao thức bảo mật trên Internet như SSL, TLS và SSH hoạt động ở tầng nào trên mô hình OSI
a.Tầng Network
b.Tầng Transport
c.Từ tầng Transport trở lên đến tầng 7
d.Tầng Session
15. Kỹ thuật tấn công phổ biến trên Web là
a. Chiếm hữu phiên làm việc.
b.Tràn bộ đệm.
c.Từ chối dịch vụ (DoS)
d.Chèn câu truy vấn SQL.
16. Các lỗ hổng bảo mật trên hệ thống là do
a. Dịch vụ cung cấp
b. Bản thân hệ điều hành
c. Con người tạo ra
d. Tất cả đều đúng

17. Cho biết câu nào đúng trong các câu sau

a. Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn

b. Chức năng chính của Firewall là kiểm sóat luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập

c. Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm

d. Tất cả đều đúng

18. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên (session) của mô hình OSI

a. Packet filtering firewall

b. Circuit level firewall

c. Application level firewall

d. Stateful multilayer inspection firewall

19.Những giao thức WAN nào có thể được định hình trên một kết nối tuần tự không đồng bộ (Chọn 2)

a. PPP

b. ATM

c. HDLC

d. SDLC

20. Khi thuê một giải pháp VPN, những loại tấn công nào bạn cần phải xét đến ?

a. Denial of Service (DoS) attacks, Internet Viruses..

b. Distributed Denial of Service (DDoS) attacks.

c. Data confidentiality, IP Spoofing.

d. Network mapping, Internet Viruses.

21. Các phát biểu sau đây phát biểu là là đúng nhất

a.Fire wal là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công

b.Là một điểm chặn của trong quá trình điều khiển và giám sát.

c. Là một phần mềm hoặc phần ứng có khả năng ngăn chặn tấn công từ bên trong và bên ngoài vào hệ thống.

d.Là một giải pháp giúp hệ thống phát hiện và ngăn chặn các truy cập trái phép

22. Bảo mật thư điện tử là nhằm đảm bảo

a.Tính tin cẩn (confidentiality), Tính xác nhận,Toàn vẹn thông điệp(integrity), Sự thối thác ban đầu (non-repudiation of origin)

b. Tính xác nhận,Toàn vẹn thông điệp(integrity), Sự thối thác ban đầu (non-repudiation of origin), tính bền vững

c.Sự thối thác ban đầu (non-repudiation of origin), tính bền vững, tính ổn khi gởi và nhận

d.Tất cả đều đúng

23. Các giao thức được để bảo mật thư điện tử là

a.GPG, S/MINE

b.SHA-1, S/MINE

c.CAST-128 / IDEA/3DES

d. Keboros, X.509

24. Chữ ký điện tử (digital signature) sử dụng thuật tóan nào sau đây

a. RSA,MD5

b. RSA,MD5, Keboros

c. MD5, SHA,RSA

d.Không dùng thuật tóan nào nêu trên

25. Chữ ký điện tử là

a.Là một chuỗi đã được mã hóa theo thuật tóan băm và đính kèm với văn bản gốc trước khi gởi.

b.Đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

c.a và b đều đúng

d.Tất cả cả đều sai

26. Các bước mã hóa của chứ ký điện tử

a.Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, Sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu.

b.Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu và nén dữ liệu gởi đi.

c.Chỉ sử dụng giải thuật băm để thay đổi thông điệp cần truyền đi và sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên.

d.Tất cả đều đúng

27. Các bước kiểm tra của chứ ký điện tử

a. Gồm các bước

1.Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message,

2.Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm, So sánh kết quả thu được ở bước 1 và 2.

3.Nếu trùng nhau, ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của người gửi.

b.Chỉ có bước 1 và 2

c.Gồm các bước

1.Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message,

2.Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm, So sánh kết quả thu được ở bước 1 và 2.

3.Nén dữ liệu rồi gởi đi

d.Không có bước nào ở trên là đúng

28. Việc xác thực người dùng khi đăng cập vào hệ thống Window XP, 2000 hoặc 2003 sử dụng giải thuật

a.RSA

b.Keberos

c.MD5

d.SHA

29. Để thực hiện tấn công bằng Trojan, kẻ tấn công chỉ cần

a.Tạo 1 file chạy (*.exe, *.com) vận hành trên máy nạn nhân là đủ

b. Cho máy nạn nhân lây nhiễm một loại virus bất kỳ nào đó.

c. Thực hiện đồng thời 2 file, một file vận hành trên máy nạn nhân, file còn lại hoạt động điều khiển trên máy kẻ tấn công.

d. Không có điều nào đúng.

30. Giao thức bảo mật IPSec hoạt động ở tầng

a. Chỉ ở tầng transport ở mô hình OSI

b.Từ tầng 4 tới tầng 7 ở mô hình OSI

c.Network Layer ở mô hình OSI

d.Tất cả đều sai

31. Cho biết phát biểu sau đây phát biểu nào là đúng nhất về registry

a.Regỉstry là một cơ sở dữ liệu dùng để lưu trữ thông tin về những sự thay đổi, những lựa chọn, những thiết lập từ người sử dụng Windows.

b.Regỉstry là một phần mềm tiện ích hỗ trợ cho người dùng thay đổii cấu hình Window khi cần thiết

c. Regỉstry là một thành phần của hệ điều hành Window

d. Tất cả đều đúng

32.Có bao nhiêu kiểu dữ liệu trong Registry

a. 5 b. 4 c. 6 d. 7

33. Các kiểu dữ liệu dùng trong registry là

a.interger, real,text,string

b.HKEY_CLASSES_ROOT, -USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, HKEY_DYN_DATA

c.HKEY_CLASSES_ROOT, -USER, HKEY_LOCAL_MACHINE, REG_BINARY

d.REG_BINARY, REG_DWORD, REG_EXPAND_SZ, REG_MULTI_SZ, REG_SZ

34. Để ẩn tất cả các ổ đĩa trong registry (A,B,C,D…) thì biến REG_DWORD trong Userkey và Systemkey có giá trị là bao nhiêu

a. 65656000

b. 67188270

c. 67108863

d.Tất cả đều sai

35. Để sử dụng xác thực Keberos V5 ở tất cả máy trạm Window98, người ta thực hiện :

a. Update window 98 lên XP hoặc Window 2000

b. Cài đặt tiện ích Distributed Security Client trên tất cả các máy chạy Window 98

c. Chỉ cần cài đặt Active Directory trên Server hệ thống

d. Không thể thực hiện được

36. Khi cài đặt Window 2000 Server trên hệ thống NTFS, nhưng không thấy có hiển thị mục Security ở Security tables vì ?

a. Update Window 2000 mà không remote trước khi cài đặt

b. Cài đặt Window 2000 nhiều lần trên Server

c. Bản Window 2000 không có bản quyền

d. Tất cả đều đúng
37. Dịch vụ Active Directory thực hiện các chức năng sau
a. Tổ chức và xây dựng các domain; xác thực và cấp quyền cho các đối tượng
b. Duy các hoạt động của các dịch vụ bảo mật cho Window Server và xác thực, cấp quyền cho các đối tượng
c. Chỉ thực hiện việc xác thực và cấp các quyền cho users và groups
d. Quản lý tài nguyên và người dùng; xác thực và cấp các quyền cho users và groups; giám sát hoạt động của các user
38. Thuật tóan thực hiện trong cơ chế bảo mật IP (IP Sec) ở Window sử dụng là
a.MD5 và SHA1
b. Kerberos và DES
c. DES hoặc 3DES (triple DES).
d.Tất cả đều sai
39. Trong Window 98,XP Registry được lưu trữ ở đâu ?
a.Được lưu trong file Classes.dat trong thư mục Windows
b.Được lưu trong thư mục "Windows System32 Config
c.Trong 2 file: user.dat và system.dat trong thư mục Windows
d.Tất cả đều sai
40. Để thực hiện sửa đổi cấu hình trên registry ta thực hiện như sau:
a. Gõ regedit vào cửa sổ Run
b. Bấm Ctrl+ Esc+ r rồi bấm Enter
c. a và b đúng
d.Tất cả đều sai
41.Quy trình crack một sản phẩm phần mềm đơn giản gồm mấy bước
a. 3 b.4 c.5 d.3 hoặc 4
42. Hai giao thức sử dụng trong IPSec (IPSec Protocol) gồm
a.IP Authentication Header, TCP/IP
b.TCP/IP, IP Encapsulating Security Payload
c.IP Authentication Header, IP Encapsulating Security Payload
d.Tất cả đều đúng
43. Các điểm khác nhau cơ bản giữa dịch vụ X.509 và Kerberos là
a. Dựa trên mã hóa đối xứng
b. Được sử dụng trong dịch vụ mail
c. Xác thực nhiều chiều
d. Tất cả đều đúng
44. Các chức năng cơ bản của kỹ thuật tấn công Sniffer
a. Tự động chụp các tên người sử dụng (Username) và mật khẩu không được mã hoá, Chuyển đổi dữ liệu trên đường truyền, phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng.
b. Bắt gói tin trên đường truyền, phân tích lỗi và giải mã gói tin
c. Bắt gói tin trên đường truyền, mã hóa vag giải mã dữ liệu
d.Tất cả đều đúng
45. Các bước tấn công của Web Server theo trình tự sau :
a. Thăm dò, Scan, Giành quyền truy cập, Duy trì truy cập, Xóa vết

b. Scan, Thăm dò, Giành quyền truy cập, Duy trì truy cập, Xóa vết

c. Thăm dò, Scan, Duy trì truy cập, Giành quyền truy cập, Xóa vết

d. Giành quyền truy cập, Duy trì truy cập, Scan, Thăm dò

46. Hiện tượng này do loại chương trình nguy hiểm nào gây ra : Làm mất một số file, làm phân mãnh ổ đĩa, gây tác hại vào những ngày, tháng đặc biệt v.v…

a. Virrus,Zombie b. Worm, Virus **c. Logicbomb, Virus** d.Trapdoors, Trojan

47.Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố sau :

a.Khởi sự, Cách thực hiện, biểu hiện mà nó ghi nhận

b.Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp

c. Cách thực hiện, biểu hiện mà nó ghi nhận, những đặc trưng ghép nối hoặc tích hợp

d.Tất cả đều đúng

48. Hai cơ chế chính của hệ thống IDS Trigger để phát hiện khi có một kẻ xâm nhập tấn công mạng là :

a.Phát hiện biểu hiện không bình thường, phát hiện sử dụng không đúng

b.Phát hiện hiện tượng trùng lặp, phát hiện không bình thường

c. Phát hiện thay đổi, phát hiện sử dụng bất bình thường

d.Tất cả đều đúng

49.Mục tiêu là phân tích mật mã là gì?

a. Để xác định thế mạnh của các thuật toán một

b. Để tăng cường chức năng thay thế trong một thuật toán mật mã

c. Để giảm chức năng transposition trong một thuật toán mật mã

d. Để xác định hoán vị sử dụng

50. Điều gì sẽ xãy ra khi một thông báo đã được sửa đổi?

a. Khoá công cộng đã được thay đổi

b. Chìa khóa cá nhân đã được thay đổi

c. Thông điệp số đã được thay đổi

d.Tin nhắn đã được mã hóa đúng cách

51.Mà hóa nào sau đây là một tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn?

a. Data Encryption Standard

b. Digital Signature Standard

c. Secure Hash Algorithm

d. Chữ kí dữ liệu tiêu chuẩn

52.Nếu kẻ tấn công lấy trộm một mật khẩu có chứa một chiều mật khẩu đã mật mã, loại tấn công, cô sẽ thực hiện để tìm mật khẩu đã mật mã?

a. Tấn công Man-in-the-middle

b. Tấn công Birthday

c. Tấn công Denial of Service

d. Tấn công Dictionary

53.Lợi thế của RSA là gì so với DSS?

a.Nó có thể cung cấp cho chữ ký số và mã hóa các chức năng

b.Nó sử dụng nguồn tài nguyên ít hơn và mã hóa nhanh hơn bởi vì nó sử dụng các phím đối xứng

c.Nó là một thuật toán mật mã khối so với một thuật toán mật mã dòng

d.Nó sử dụng một lần mã hóa pad

54.Những gì được sử dụng để tạo ra một chữ ký điện tử?
a. Khóa riêng của người nhận
b. Khóa công khai của người gửi
c. Khóa riêng của người gửi
d. Khóa công khai của người nhận
55. Phương thức nào sau đây là tốt nhất mô tả một chữ ký điện tử?
a. Một phương thức chuyển giao một chữ ký viết tay vào một tài liệu điện tử
b. Một phương pháp mã hóa thông tin bí mật
c. Một phương pháp để cung cấp một chữ ký điện tử và mã hóa
d. Một phương pháp để cho những người nhận của tin nhắn chứng minh nguồn gốc và sự toàn vẹn của một tin nhắn
56. Sử dụng nhiêu bit với DES để có hiệu quả?
a.56 b.64 c.32 d.16
57.Các yếu tố ảnh hưởng đến quá trình mã hóa
a. Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền
b. Thời gian thực hiện mã hóa và giải mã
c. Thực hiện mã hóa khối, mở rộng số bít xử lý
d. Tất cả đều sai
58. Đối với Firesall lọc gói, hình thức tấn công nào sau đây được thực hiện
a. Nhái địa chỉ IP, tấn công giữa, tấn công biên
b. Nhái địa chỉ IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ
c. Nhái địa chỉ IP, tấn công vượt firewall,tấn công từng mẫu nhỏ
d. Nhái địa chỉ IP, tấn công vượt firewall, tấn công đường đi nguồn
59.Ai là người tham gia vào việc phát triển đầu tiên hệ thống mã hóa khóa công?
a. Adi Shamir
b. Ross Anderson
c. Bruce Schneier
d. Martin Hellman
60. DES là viết tắt của từ nào ?
a. Data encryption system
b. Data encryption standard
c. Data encoding standard
d. Data encryption signature
61. Các phát biểu sau đây, phát biểu nào tốt nhất mô tả một hacker mũ trắng?
A. Chuyên gia bảo mật
B. Cựu Hacker mũ đen
C. Cựu Hacker mũ xám
D. Hacker hiểm độc
62. Giai đoạn đầu của hacking là gì?
A. Duy trì truy cập
B. Gaining truy cập
C. Trinh sát
D. Dò tìm (Scanning)

63. Khi một hacker cố gắng tấn công một máy chủ qua Internet nó được gọi là loại tấn công?

A. Tấn công từ xa

B. Tấn công truy cập vật lý

C. Truy cập địa phương

D. Tấn công tấn công nội

64. Công cụ nào sau đây đúng là một công cụ để thực hiện footprinting không bị phát hiện?

A. Whois search

B. Traceroute

C. Ping sweep

D. Host scanning

65. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì?

A. Scanning

B. Enumeration

C. System hacking

D. Active information gathering

66. Footprinting là gì?

A. đo dấu vết của một hacker có đạo đức

B. tích luỹ dữ liệu bằng cách thu thập thông tin về một mục tiêu

C. quét một mạng lưới mục tiêu để phát hiện hệ điều hành các loại

D. sơ đồ bố trí vật lý của một mạng của mục tiêu

67. Lý do tốt nhất để thực hiện một chính sách bảo mật là gì?

A. Tăng an ninh.

B. Nó làm cho khó hơn việc thi hành bảo mật.

C. Hạn chế quyền hạn của nhân viên

D. Làm giảm an ninh.

68. FTP sử dụng cổng gì ?

A. 21

B. 25

C. 23

D. 80

69. Cổng nào được HTTPS sử dụng?

A. 443

B. 80

C. 53

D. 21

70. Trojan Horse là gì?

A. một chương trình độc hại mà lấy cắp tên người dùng và mật khẩu của bạn

B. gây hại như mã giả mạo hoặc thay thế mã hợp pháp

C. Một người sử dụng trái phép những người thu truy cập vào cơ sở dữ liệu người dùng của bạn và cho biết thêm mình như một người sử dụng

D. Một máy chủ đó là phải hy sinh cho tất cả các hacking nỗ lực để đăng nhập và giám sát các hoạt động hacking

71. John muốn cài đặt một ứng dụng mới vào máy chủ của Windows 2000.
Ông muốn đảm bảo rằng các ứng dụng bất kỳ ông sử dụng chưa được cài Trojan.
Ông có thể làm gì để giúp đảm bảo điều này?
A. So sánh chữ ký MD5 của tập tin với một trong những công bố trên các phương tiện truyền thông phân tán
B. Xin các ứng dụng thông qua SSL
C. So sánh chữ ký virus của file với một trong những công bố trên các phương tiện truyền thông
D. Cài đặt các ứng dụng từ đĩa CD-ROM
72. Hầu hết các lỗi SQL Injection đều là do (chọn 2 phương án)
a. câu lệnh SQL sai
b. trình duyệt Web không hỗ trợ
c. User làm cho câu lệnh SQL sai
d. Sử dụng Hệ quản trị CSDL không có bản quyền
73. Chính sách bảo mật là
a. Cơ chế mặc định của hệ điều hành
b. phương thức xác định các hành vi "phù hợp" của các đối tượng tương tác với hệ thống
c. các tập luật được xây dựng nhằm bảo vệ các tấn công bất hợp pháp từ bên ngoài
d. Tất cả đều đúng
74. Các loại mục tiêu của chiến tranh thông tin
a. Website, E-commerce server
b. Internet Relay Chat (IRC), Domain Name System (DNS)
c. ISP, Email server
d. Tất cả đều đúng
75. Khi thực hiện triển khai HIDS khó khăn gặp là
a. Chi phí lắp đặt cao, khó bảo quản và duy trì
b. Giới hạn tầm nhìn mạng, phải xử lí với nhiều hệ điều hành khác trên mạng.
c. Thường xuyên phải cập nhật bảng vá lỗi
d. Thường xuyên cài đặt lại phải khi hệ thống mạng thay đổi hệ điều hành