1. Những chữ đầu của nhóm từ ACL là tên viết tắt của:
A. Arbitrary Code Language
B. Access Control Library
C. Access Control List
D. Allowed Computer List
2. Nên cài mức truy cập mặc định là mức nào sau đây?
A. Full access
B. No access
C. Read access
D. Write access
3. Sau khi một user được định danh và xác thực hệ thống, để cho phép user sử dụng tài nguyên bạn phải thực hiện điều gì?
A. Phải được ủy quyền
B. Được truyền lại
C. Được mã hóa
D. Được enable
4. Quyền truy cập nào cho phép ta lưu giữ một tập tin?
A. Đọc
B. Sao chép
C. Hiệu chỉnh
D. Ghi
5. Quyền truy cập nào cho phép ta hiệu chỉnh thuộc tính của một tập tin?
A. Hiệu chỉnh (Modify)
B. Sao chép (Copy)
C. Thay đổi (Change)
D. Biên tập ( Edit)
6. Các quyền truy cập tối đa nên dành cho user là gì ?
A. Ít nhất là quyền đọc và ghi
B. Không có quyền truy cập
C. Đủ để thực hiện công việc theo chức trách
D. Toàn quyền
7. Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?
A. Disable tài khoản không dùng đến
B. Hạn chế thời gian
C. Ngày hết hạn tài khoản
D. Giới hạn số lần logon
8. Sau khi một user đã được định danh (identifed), điều gì cần phải làm trước khi họ log vào một mạng máy tính ?
A. Xác thực với mật khẩu
B. Họ phải nhập user ID đã được mã hóa

C. Được phép truy cập với mức ưu tiên được thiết lập .
D. Người quản trị phải enable để gõ vào
9. Chiều dài tối thiểu của mật khẩu cần phải là :
A. 12 đến 15 ký tự
B. 3 đến 5 ký tự
C. 8 ký tự
D. 1 đến 3 ký tự
10. Điều gì cần được thực hiện đối với tập tin mật khẩu để ngăn chặn một người dùng trái phép crack vào các nội dung ?
A. Hủy bỏ tất cả các quyền truy cập
B. Mã hóa tập tin mật khẩu
C. Di chuyển ngoại tuyến đến một đĩa mềm
D. Sao chép đến một tập tin bù nhìn với một tên khác
11. Một IP flood theo các host phát tán trực tiếp đến một Web server là một ví dụ của loại tấn công gì ?
A. Trojan Hors
B. Sâu
C. Tấn công IP
D. DoS phân tán (DDoS)
12. Để ngăn tấn công DoS, một quản trị mạng chặn nguồn IP với tường lửa, nhưng tấn công vẫn tiếp diễn. Điều gì có khả năng xảy ra nhất ?
A. Sâu DoS đã lây nhiễm cục bộ
B. Tấn công đang đến từ nhiều host (DDoS)
C. Một tường lửa không thể ngăn chặn tấn công DoS
D. Phần mềm Antivirus cần được cài đặt trên máy chủ đích
13. Cách bảo vệ nào sau đây là tốt nhất để chống lại tấn công DoS kiểu làm tràn băng thông và bộ đệm của hệ thống .
A. Subnet mask
B. Cài đặt phần mềm bảo vệ Antivirus
C. Disable web server
D. Chặn giao thức ICMP
14. Các loại khoá mật mã nào sau đây dễ bị crack nhất ?
A. 128 bit
B. 40 bit
C. 256 bit
D. 56 bit
15. Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm HĐH ?
A. Cài đặt bản service pack mới nhất
B. Cài đặt lại HĐH thông dụng
C. Sao lưu hệ thống thường xuyên

D. Shut down hệ thống khi không sử dụng
16. Các mật khẩu nào sau đây là khó phá nhất đối với một hacker ?
A. password83
B. reception
C. !$aLtNb83
D. LaT3r
17. Một người dùng đã mua một máy tính xách tay đã nhiễm virus.Trên máy không chứa phần mềm Antivirus và chưa được kết nối với mạng.Cách tốt nhất để sửa chữa máy tính xách tay là gì ?
A. Nối mạng máy tính xách tay và download phần mềm antivirus từ máy chủ
B. Khởi động máy tính xách tay với đĩa antivirus
C. Nối mạng máy tính xách tay và download phần mềm antivirus từ Internet
D. Kết nối máy tính xách tay đến một máy tính cá nhân khác và diệt virus từ đó
18. Các tập tin nào sau đây có khả năng chứa virus nhất ?
A. database.dat
B. bigpic.jpeg
C. note.txt
D. picture.gif.exe
19. Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi một hoạt động nào đó được kích hoạt ?
A. Sâu
B. Ngựa trojan
C. Logic bomb
D. Stealth virus
20. Trong suốt quá trình kiểm định một bản ghi hệ thống máy chủ, các mục nào sau đây có thể được xem như là một khả năng đe dọa bảo mật ?
A. Năm lần nỗ lực login thất bại trên tài khoản "jsmith"
B. Hai lần login thành công với tài khoản Administrator
C. Năm trăm ngàn công việc in được gởi đến một máy in
D. Ba tập tin mới được lưu trong tài khoản thư mục bởi người sử dụng là "finance"
21. Phương pháp thông tin truy cập từ xa nào được xem như kết nối điển hình đến Internet mọi lúc, nó làm gia tăng rủi ro bảo mật do luôn mở đối với mọi cuộc tấn công ?
A. Cable modem & DSL
B. Dial-up
C. Wireless
D. SSH
22. Tính năng bảo mật nào có thể được sử dụng đối với một máy trạm quay số truy cập từ xa sử dụng một username và mật khẩu ?
A. Mã hóa số điện thoại
B. Kiểm tra chuỗi modem

C. Hiển thị gọi
D. Gọi lại ( Call back)
23. Tiện ích nào sau đây là một phương thức bảo mật truy cập từ xa tốt hơn telnet ?
A. SSL
B. SSH
C. IPSec
D. VPN
24. Các giao thức đường h`ầm nào sau đây chỉ làm việc trên các mạng IP ?
A. SLIP
B. IPX
C. L2TP
D. PPTP
25. Mục đích của một máy chủ RADIUS là
A. Packet Sniffing
B. Mã hóa
C. Xác thực
D. Thỏa thuận tốc độ kết nối
26. Các giao thức xác thực nào sau đây được sử dụng trong các mạng không dây ?
A. 802.1X
B. 802.11b
C. 802.11a
D. 803.1
27. Các giao thức nào sau đây làm việc trên lớp IP để bảo vệ thông tin IP trên mạng ?
A. IPX
B. IPSec
C. SSH
D. TACACS+
28. LAC ( L2TP Access Control) và LNS ( L2TP Network Server)) là các thành ph`ần của giao thức đường h`ầm nào ?
A. IPSec
B. PPP
C. PPTP
D. L2TP
29. Giao thức được sử dụng rộng rãi nhất để truy cập kiểu quay số đến một máy chủ từ xa là
A. SLIP
B. PPP
C. RAS
D. Telnet
30. Kỹ thuật nào được sử dụng để bảo đảm thông tin liên lạc qua một mạng không được bảo mật ?

A. Telnet
B. SLIP
C. VPN
D. PPP
31. Các thiết bị nào sau đây có thể sử dụng được trên mạng không dây ?
A. Máy vi tính để bàn
B. Máy tính xách tay
C. PDA
D. Tất cả các loại trên
32. Thiết bị nào được sử dụng để cho phép các máy trạm không dây truy cập vào một mạng LAN rộng ?
A. 802.11b
B. Tường lửa
C. Điểm truy cập không dây (Wiless Access Point)
D. VPN
33. Các chuẩn giao thức mạng không dây nào sau đây phân phối nội dung Wireless Markup Language (WML) đến các ứng dụng Web trên các thiết bị c`ầm tay (PDA)?
A. WAP
B. WEP
C. 802.11g
D. SSL
34. Các chuẩn giao thức mạng không dây IEEE nào sau đây là phổ biến nhất ?
A. 803.11b
B. 802.11g
C. 802.11a
D. 802.11b
35. Mức mã hóa WEP nào nên được thiết lập trên một mạng 802.11b ?
A. 128 bit
B. 40 bit
C. 28 bit
D. 16 bit
36. Cơ cấu bảo mật mạng không dây nào sau đây là ít an toàn nhất ?
A. VPN
B. Mã hóa WEP 40 bit
C. Bảo mật định danh mạng
D. Mã hóa WEP 128 bit
37. Bộ lọc địa chỉ MAC được định nghĩa như :
A. Được phép truy cập đến một địa chỉ MAC nhất định.
B. Ngăn chặn truy cập từ một địa chỉ MAC nhất định.
C. Mã hóa địa chỉ MAC của thiết bị không dây.
D. Tường lửa cá nhân

38. Phương pháp điều khiển truy cập có hiệu quả và an toàn nhất đối với mạng không dây là:
A. Mã hóa WEP 40 bit
B. VPN
C. Mã hóa WEP kết hợp với lọc địa chỉ MAC
D. Nhận dạng bảo mật mạng
39. Cơ cấu bảo mật nào sau đây được sử dụng với chuẩn không dây WAP ?
A. WTLS
B. SSL
C. HTTPS
D. Mã hóa WEP
40. Thiết bị nào sử dụng bộ lọc gói và các quy tắc truy cập để kiểm soát truy cập đến các mạng riêng từ các mạng công cộng , như là Internet ?
A. Điểm truy cập không dây
B. Router
C. Tường lửa
D. Switch
41. Thiết bị nào cho phép ta kết nối đến một mạng LAN của công ty qua Internet thông qua một kênh được mã hóa an toàn ?
A. VPN
B. WEP
C. Modem
D. Telnet
42. Ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng ?
A. IDS
B. FTP
C. Router
D. Sniffer
43. Cần phải làm gì để bảo vệ dữ liệu trên một máy tính xách tay nếu nó bị lấy cắp ?
A. Khóa đĩa mềm
B. Enable khi login và tạo mật khẩu trên HĐH
C. Lưu trữ đều đặn trên CD-ROM
D. Mã hóa dữ liệu
44. Ta phải làm gì để ngăn chặn một ai đó tình cờ ghi đè lên dữ liệu trên một băng từ ?
A. Xóa nó bằng nam châm
B. Dán nhãn cẩn thận
C. Thiết lập tab “Write-protect ” .
D. Lưu giữ nó tại chỗ
45. Phương tiện nào sau đây không bị ảnh hưởng bởi từ tính ?

A. Đĩa mềm
B. CD-ROM
C. Flash card
D. Băng từ
46. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực ?
A. PIN
B. Quét võng mạc
C. Mã hóa khóa
D. Thẻ nhớ
47. Loại media nào sau đây không phải là một thiết bị cơ động được ?
A. Đĩa mềm
B. Ổ đĩa đĩa CD
C. Thẻ thông minh
D. Băng từ
48. Các thiết bị hay các ứng dụng bảo mật nào sau đây nên được sử dụng để theo dõi và cảnh báo các quản trị mạng về truy cập trái phép ?
A. Chương trình Antivirus
B. Switch
C. Hệ thống phát hiện xâm nhập (IDS)
D. Dụng cụ phân tích mạng
49. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như là web, FTP, và các máy chủ email ?
A. DMZ
B. VLAN
C. VPN
D. Intranet
50. Loại mạng nào mô tả cấu hình mạng bên trong của một công ty dùng cho mô hình kinh doanh B2B ( Business to Business) ?
A. VLAN
B. Intranet
C. Extranet
D. VPN
51. Dịch vụ mạng nào cho phép các địa chỉ mạng bên trong được "che dấu"( hidden) khỏi các mạng bên ngoài và cho phép vài host của mạng bên trong sử dụng các địa chỉ trùng với mạng bên ngoài ?
A. NAT
B. VPN
C. VLAN
D. IP spoofing
52. Công nghệ nào được sử dụng để chia một mạng bên trong thành mạng logic nhỏ hơn, dễ sử dụng hơn ?

A. NAT
B. Tunneling
C. VPN
D. VLAN
53. Không sử dụng một liên kết chuyên dụng , phương pháp tốt nhất để kết nối hai mạng được định vị trong các văn phòng có khoảng cách địa lý xa nhau là gì ?
A. VLAN
B. Tường lửa
C. DMZ
D. VPN
54. Sau khi cố gắng login đến một trạm làm việc trong 3 lần, một user thấy đã bị khóa bên ngoài hệ thống và không thể thực hiện bất kỳ nổ lực nào hơn nữa. Vấn đề này phù hợp nhất với điều gì ?
A. Cổng mạng disable
B. Tường lửa disable khi truy cập đến host
C. User quên mật khẩu của họ
D. Hệ thống phát hiện xâm nhập disable tài khoản của user
55. Đặc tính nào của các thiết bị mạng như router hay switch, cho phép điều khiển truy cập dữ liệu trên mạng ?
A. Giao thức DNS
B. Cập nhật vi chương trình ( Firmware)
C. Tường lửa
D. Danh sách điều khiển truy cập (ACL)
56. Phần nào của một thiết bị phần cứng có thể được nâng cấp để cung cấp khả năng bảo mật tốt hơn và đáng tin hơn ?
A. Vi chương trình (firmware)
B. Quét cổng
C. Flash memory
D. Cấu hình tập tin
57. Giao thức nào sau đây cần xóa trên thiết bị mạng quan trọng như router ?
A. TCP/IP
B. ICMP
C. IPX/SPX
D. RIP
58. Các giao thức nào sau đây cần xóa trên một máy chủ email để ngăn chặn một user trái phép khai thác các điểm yếu bảo mật từ phần mềm giám sát mạng ?
A. IMAP
B. POP3
C. TCP/IP
D. SNMP
59. Điều gì cần được thực hiện với một email server để ngăn chặn user bên ngoài gởi

email thông qua nó ?
A. Cài đặt phần mềm antivirus và antispam.
B. Hạn chế chuyên tiếp tín hiệu SMTP.
C. Xoá quyền truy cập POP3 và IMAP
D. Enable login được mã hóa
60. Điều gì có thể được thiết lập trên một server DHCP để ngăn chặn các máy trạm trái phép lấy được một địa chỉ IP từ server ?
A. Quét cổng
B. Thiết lập "Danh sách truy cập thư mục LDAP"
C. Phát hiện xâm nhập
D. DNS
61. Văn bản sau khi được mã hóa, được gọi là gì ?
A. Chứng chỉ
B. Mật mã đối xứng
C. Khóa công khai
D. Văn bản mã
62. Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã ?
A. Hiệu quả
B. Bảo mật
C. Toàn vẹn
D. Không chối từ
63. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và giải mã ?
A. Không đối xứng
B. Đối xứng
C. RSA
D. Diffie-Hellman
64. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hoá dữ liệu?
A. DSA
B. ECC
C. 3DES
D. AES
65. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ?
A. Skipjack
B. Blowfish
C. Không đối xứng
D. Đối xứng
66. Các giao thức mã hóa và các thuật toán nào sau đây được sử dụng như là nền tảng

của hạ tầng cơ sở hạ tầng khóa công khai (PKI)?
A. MD4
B. SHA
C. Diffie-Hellman
D. Skipjack
67. Khi giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là gì ?
A. Tấn công vào ngày sinh
B. Xung đột
C. Chữ ký số
D. Khóa công khai
68. Thực thể nào sau đây cho phép phát hành , quản lý, và phân phối các chứng chỉ số ?
A. Quyền cấp chứng chỉ (Certificate Authority)
B. Quyền đang ký (Registation Authority)
C. Chính phủ (NSA)
D. PKI
69. Tính hợp lệ của một chứng chỉ dựa vào điều gì ?
A. Tính hợp lệ của Quyền cấp chứng chỉ (CA)
B. Tính hợp lệ của người sở hữu .
C. Tính hợp lệ của khóa công khai
D. Giai đoạn chứng chỉ được sử dụng
70. Trong một mô hình phân cấp ủy thác giữa các tổ chức chứng thực và các người dùng cuối, mô hình nào sau đây được coi là xu hướng chung của việc phát hành chứng chỉ?
A. Các chính sách thu hồi chứng chỉ
B. Các ngày hợp lệ
C. Khóa cá nhân
D. Chứng thực gốc ( Root Certificate)
71. Khi ta lưu giữ một khóa cá nhân trên đĩa cứng cục bộ, làm thế nào để bảo đảm là nó được bảo mật ?
A. Cần bảo vệ bằng mật khẩu
B. Lưu trữ dữ liệu sao lưu vào đĩa mềm
C. Lưu trữ bản sao trong bì thư
D. Lưu trữ nó trong một thư mục tương tự như khóa công khai
72. Cách nào sau đây được coi là an toàn nhất để lưu trữ một khóa cá nhân ?
A. Lưu nó trên ổ cứng ở dạng bản rõ
B. Niêm phong nó trong một bao thư và để nó trong ngăn bàn
C. Mã hóa nó trên một thẻ thông minh
D. Lưu nó trên một thiết bị USB di động ở dạng bản rõ
73. Một quản trị mạng mới đây đã bị sa thải khỏi công ty. Cần phải làm gì với chứng

chỉ hiện hành của họ ?
A. Làm mới lại đối với người quản trị mới
B. Thu hồi lại chứng chỉ
C. Đình chỉ tạm thời
D. Hết hiệu lực
74. Các phương pháp sinh trắc học nào sau đây được coi là an toàn nhất ?
A. Phân tích chữ ký
B. Lấy dấu vân tay
C. Quét tiếng nói
D. Không quan trọng
75. Khi kết thúc công việc trên máy tính xách tay và ra ngoài khoảng 1 tiếng vào buổi trưa. Ta nên làm gì trước khi ra ngoài ?
A. Nói với đồng nghiệp để mắt đến máy tính xách tay
B. Log out khỏi máy tính xách tay
C. Shut down và đóng máy lại
D. Chắc chắn rằng máy tính xách tay của ta được bảo vệ trên bàn làm việc hay được khóa trong cabin
76. Một user gọi điện đến cho ta (với tư cách là người quản lý) thông báo họ bị mất mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì ?
A. Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ
B. Tạo một login và mật khẩu tạm thời để họ sử dụng
C. Xác minh định danh của họ trước khi cấp quyền truy cập
D. Cho họ một mật khẩu riêng tạm thời
77. Trong khoảng thời gian nguồn điện bị sụt áp do quá tải bất thường, các thiết bị nào sau đây là hữu dụng nhất trong việc duy trì các mức nguồn điện thích hợp ?
A. Dự phòng nguồn điện của máy phát điện
B. UPS
C. Ổn áp
D. Thanh nguồn điện
78. Quản trị văn phòng của bạn đang được huấn luyện để thực hiện sao lưu máy chủ. Phương pháp xác thực nào là lý tưởng đối với tình huống này ?
A. MAC
B. DAC
C. RBAC
D. Các mã thông báo bảo mật
79. Phương pháp xác thực nào sử dụng một KDC để thực hiện xác thực ?
A. Chap
B. Kerberos
C. Sinh trắc học
D. Thẻ thông minh
80. Phương pháp xác thực nào gởi trả lại một "yêu cầu" (request) cho máy trạm và"

yêu c ầu" đó được mã hóa và gởi trở lại máy chủ ?
A. Kerberos
B. Các mã thông báo bảo mật
C. DAC
D. CHAP
81. Qui trình xác thực nào sử dụng nhi ều hơn một yếu tố xác thực để logon ?
A. Đa yếu tố ( multi-factor)
B. Sinh trắc học
C. Thẻ thông minh
D. Keberos
82. Các giao thức hay các dịch vụ nào sau đây nên loại bỏ trong mạng nếu có thể ?
A. Email
B. Telnet
C. WWW
D. ICMP
83. Mạng nào sau đây không phải là một vùng bảo mật ?
A. Internet
B. Intranet
C. Extranet
D. NAT
84. Các giao thức nào sau đây cho phép một tổ chức đưa một địa chỉ TCP/IP đơn lên Internet ?
A. NAT
B. VLAN
C. DMZ
D. Extranet
85. Phương pháp quét võng mạc thích hợp nhất đối với các dịch vụ nào sau đây ?
A. Kiểm định
B. Xác thực
C. Kiểm soát truy cập
D. Bảo mật dữ liệu
86. Công nghệ nào sau đây dựa vào thuộc tính vật lý của user để xác thực ?
A. Thẻ thông minh
B. Sinh trắc học
C. Xác thực lẫn nhau
D. Các mã thông báo
87. Kỹ thuật cho phép tạo kết nối ảo giữa hai mạng sử dụng một giao thức bảo mật được gọi là gì ?
A. Tunelling
B. VLAN
C. Internet

D. Extranet
88. Qui trình quyết định giá trị của thông tin hay thiết bị trong một tổ chức được gọi là gì?
A. Nhận dạng chuỗi
B. Đánh giá rủi ro
C. Đánh giá tài nguyên thông tin
D. Quét các điểm yếu
89. Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin nào sau đây sẽ giúp ích nhiều nhất ?
A. Xác minh tài sản sở hữu
B. Đánh giá rủi ro
C. Nhận dạng mối đe dọa
D. Các điểm yếu
90. Khi một user báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều gì sau đây cần làm như là bước đầu tiên để xử lý tình huống này ?
A. Kiểm tra lại tập tin diệt virus hiện hành
B. Định dạng lại đĩa cứng
C. Cài đặt lại hệ điều hành
D. Disable tài khoản email của anh ta
91. Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài ?
A. Đăng nhập hệ thống ( System logs)
B. Phần mềm antivirus
C. Kerberos
D. Sinh trắc học
92. Ta muốn cài đặt một máy chủ cung cấp các dịch vụ Web đến các máy trạm thông qua Internet. Ta không muốn để lộ mạng bên trong để tránh rủi ro. Phương pháp nào để thực hiện điều này ?
A. Cài đặt máy chủ trong mạng Intranet
B. Cài đặt máy chủ trong một DMZ
C. Cài đặt máy chủ trong một VLAN
D. Cài đặt máy chủ trong mạng Extranet
93. Phương pháp xác thực nào cung cấp tài liệu đáng tin cậy có hiệu lực trong suốt một phiên làm việc đơn ?
A. Các mã thông báo
B. Chứng chỉ
C. Thẻ thông minh
D. Kerberos
94. Loại tấn công nào làm việc truy cập của user đến các tài nguyên mạng bị từ chối ?
A. DoS
B. Sâu

C. Logic Bomb (bomb ngập lụt đường truyền)
D. Social engineering (Khai thác giao tiếp)
95. Loại tấn công nào sử dụng nhiều hơn một máy tính để tấn công nạn nhân ?
A. DoS
B. DDoS
C. Sâu
D. Tấn công UDP
96. Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền . Loại tấn công nào đã xảy ra ?
A. DoS
B. DDoS
C. Back door
D. Social engineering (Khai thác giao tiếp)
97. Nỗ lực tấn công để can thiệp vào một phiên liên lạc bằng việc thêm vào một máy tính giữa hai hệ thống được gọi là một …….?
A. Tấn công dạng "Man in the middle"
B. Tấn công cửa sau
C. Sâu
D. TCP/IP hijacking
98. Ta đã phát hiện ra một chứng chỉ đã hết hiệu lực vẫn đang được sử dụng nhiều lần để giành được quyền logon. Đây là loại tấn công nào ?
A. Tấn công dạng "Man in the middle"
B. Tấn công cửa sau
C. Tấn công chuyển tiếp (Relay Attack)
D. TCP/IP hijacking
99. Một kẻ tấn công cố gắng dùng địa chỉ IP để tạo một hệ thống khác trong mạng của ta nhằm giành quyền kiểm soát truy cập . Đây là loại tấn công nào ?
A. Tấn công dạng "Man in the middle"
B. Tấn công cửa sau
C. Sâu
D. TCP/IP hijacking
100. Một máy chủ trên mạng không chấp nhận các kết nối TCP nữa. Máy chủ thông báo rằng nó đã vượt quá giới hạn của phiên làm việc. Loại tấn công nào có thể đang xảy ra ?
A. Tấn công TCP ACK (tấn công kiểu SYNACK)
B. Tấn công smurf
C. Tấn công virus
D. TCP/IP hijacking
101. Tấn công smurf sử dụng giao thức nào để kiểm soát ?
A. TCP
B. IP

C. UDP
D. ICMP
102. Tổ đặc trách thông báo rằng họ đã nhận một cuộc gọi khẩn cấp từ phó chủ tịch đêm qua yêu cầu logon vào ID và mật khẩu của ông ta. Đây là loại tấn công gì ?
A. Giả mạo
B. Tấn công chuyển tiếp
C. Social engineering (Khai thác giao tiếp)
D. Trojan
103. Hệ thống của bạn đã ngừng phản ứng lại với các lệnh của bàn phím. Lưu ý rằng điều này xảy ra khi mở bảng tính và đã quay số qua internet. Loại tấn công nào có thể đã xảy ra ?
A. Logic Bomb
B. Sâu
C. Virus
D. Tấn công ACK
104. Loại virus tự che giấu nó bằng cách ẩn trong mã nguồn của các phần mềm antivirus được gọi là gì ?
A. Armored virus
B. Polymorphic virus
C. Sâu
D. Stealth virus (Virus ẩn danh)
105. Một virus được đính kèm chính nó vào boot sector của đĩa cứng và thông báo thông tin sai về kích thước các tập tin được gọi là gì ?
A. Virus Trojan
B. Stealth virus (virus ẩn danh)
C. Sâu
D. Polymorphic virus
106. Một chương trình nằm trong một chương trình khác được cài vào hệ thống gọi là một …….
A. Trojan Horse
B. Polymorphic virus
C. Sâu
D. Armored virus
107. Các user nội bộ báo cáo hệ thống của họ bị lây nhiễm nhiều lần. Trong mọi trường hợp virus có vẻ là cùng một loại. Thủ phạm thích hợp nhất là gì ?
A. Máy chủ có thể là vật mang virus
B. Ta có một sâu virus
C. Phần mềm antivirus của ta bị sự cố
D. Tấn công DoS đang thực hiện
108. Các log file trên hệ thống của bạn phát hiện một nỗ lực giành quyền truy cập đến một tài khoản đơn. Nỗ lực này đã không thành công vào thời điểm đó. Theo kinh

nghiệm của bạn thì loại tấn công thích hợp nhất là gì ?
A. Tấn công đoán mật khẩu (Password Guessing)
B. Tấn công cửa sau
C. Tấn công bằng sâu
D. TCP/IP hijacking
109. Một user báo cáo là anh ta đang nhận một lỗi chỉ ra rằng địa chỉ TCP/IP của anh ta đã bị sử dụng khi anh ta bật máy tính. Tấn công nào có thể đang thực hiện ?
A. Tấn công dạng "Man in the middle"
B. Tấn công cửa sau
C. Sâu
D. TCP/IP hijacking
110. Một đêm làm việc khuya và bạn phát hiện rằng ổ cứng của bạn hoạt động rất tích cực mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi ngờ điều gì?
A. Khả năng ổ đĩa ngừng hoạt động sắp xảy ra
B. Một virus đang phát tán rộng trong hệ thống
C. Hệ thống của bạn đang chịu tác động của tấn công DoS
D. Tấn công TCP/IP hijacking đang cố gắng thực hiện
111. Bản ghi lỗi hệ thống email của bạn báo cáo một số lượng lớn các nỗ lực logon không thành công. Loại tấn công nào có thể đang xảy ra ?
A. Tấn công khai thác phần mềm (Software exploitation attack)
B. Tấn công cửa sau ( Back door Attack))
C. Sâu (Worm)
D. TCP/IP hijacking
112. Bộ lọc gói thực hiện chức năng nào ?
A. Cho phép tất cả các gói đi vào mạng
B. Cho phép tất cả các gói rời mạng
C. Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài
D. Loại trừ sự xung đột trong mạng
113. Thiết bị nào lưu trữ thông tin về đích đến trong mạng ?
A. Hub
B. Modem
C. Firewall
D. Router
114. Giao thức nào được sử dụng rộng rãi hiện nay như là một giao thức truyền tải đối với các kết nối quay số trên Internet ?
A. SLIP
B. PPP
C. PPTP
D. L2TP
115. Giao thức nào sau đây không phù hợp đối với các kết nối VPN WAN ?

A. PPP
B. PPTP
C. L2TP
D. IPSec
116. Giao thức nào sau đây tuy không phải là một giao thức đường hầm nhưng nó sử dụng các giao thức đường hầm để bảo mật trên mạng?
A. IPSec
B. PPTP
C. L2TP
D. L2F
117. Một socket là sự kết hợp của các thành phần nào ?
A. IP và session number
B. IP và port number
C. TCP và port number
D. UDP và port number
118. Thiết bị nào giám sát lưu lượng mạng theo cách thụ động ?
A. Sniffer
B. IDS
C. Firewall
D. Web browser
119. Hệ thống nào chủ động thực hiện việc giám sát mạng, phân tích và có thể thực hiện các bước phòng ngừa , bảo vệ mạng ?
A. IDS
B. Sniffer
C. Router
D. Switch
120. Hệ thống nào được cài đặt trên Host để cung cấp một tính năng IDS ?
A. Network sniffer
B. N-IDS (Network-based IDS)
C. H-IDS (Host-based IDS)
D. VPN
121. Khi kết nối giữa các thiết bị không dây đã hoàn tất , giao thức nào được sử dụng?
A. WEP
B. WTLS
C. WAP
D. WOP
122. Giao thức nào hoạt động trên 2.4GHz và có một dải băng thông rộng 1Mbps hay 2Mbps ?
A. 802.11
B. 802.11a

C. 802.11b
D. 802.11g
123. Giao thức nào được thiết kế để cung cấp bảo mật cho mạng không dây tương đương với việc bảo mật của một mạng diện rộng ?
A. WAP
B. WTLS
C. WEP
D. IR
124. Điểm yếu nào sau đây là chủ yếu của môi trường mạng không dây ?
A. Phần mềm giải mã (Decryption software)
B. IP spoofing (Giả mạo IP)
C. A gap in the WAP (Một khe hở trong WAP)
D. Định vị nơi làm việc (Site survey)
125. Nếu ta muốn xác thực chữ ký của một người khác, khóa nào phải được sử dụng?
A. Khóa công khai của bạn .
B. Khoá cá nhân của bạn .
C. Khoá cá nhân của người cần xác thực .
D. Khoá công khai của người cần xác thực .
126. Có thể sử dụng mật mã để nhận biết tài liệu đã bị thay đổi hay không ?
A. A: Có
B. B: Không
127. Chữ ký số được sử dụng cho mục đích gì?
A. Để bảo mật tài liệu sao cho người ngoài không đọc được
B. Để kiểm tra định danh người gửi
C. Cung cấp chứng chỉ
D. Thu hồi một chứng chỉ
128. Nếu muốn xem một tài liệu "bảo mật"được mã hóa trên hệ mật bất đối xứng do người khác gởi đến , bạn phải sử dụng khóa nào để giải mật tài liệu?
A. Khoá công khai của bạn
B. Khoá công khai của bên gửi
C. Khoá cá nhân của bên gửi
D. Khoá cá nhân của bạn
129. Nếu ta muốn ký một tài liệu và sau đó gởi đến một người khác, khóa nào phải được sử dụng?
A. Khoá công khai của bạn
B. Khoá công khai của bên nhận
C. Khoá cá nhân của bên nhận
D. Khoá cá nhân của bạn
130. Bạn nhận được một email từ Microsoft, trong đó có một file đính kèm. Trong thư nói rằng có một số lỗi đã được phát hiện và sửa chữa , bạn phải chạy chương trình được đính kèm trong thư để sửa những lỗi đó. Trong trường hợp này bạn sẽ làm

gì để bảo đảm an toàn?
A. Lưu chương trình đó lại và dùng chương trình diệt virus để quét, nếu không phát hiện thấy virus, sẽ chạy chương trình đó để sửa lỗi.
B. Mở chương trình và chạy nó ngay. Chương trình đó thật sự an toàn vì nó được gửi từ Microsoft
C. Xoá email đó ngay. Mocrosoft và các nhà cung cấp không bao giờ gửi chương trình sửa lỗi qua email.
D. ...
131. Hệ mật DES sử dụng khối khoá được tạo bởi :
A. 56 bit ngẫu nhiên
B. 64 bit ngẫu nhiên
C. 128 bit ngẫu nhiên
D. 56 bit ngẫu nhiên và 8 bit kiểm tra "Parity"
132. Hệ mật DES xử lý từng khối " plain text " có độ dài :
A. 56 bit
B. 32 bit
C. 64 bit
D. 48 bit
133. Thuật giải SHA là :
A. Hàm băm một chi ều
B. Dùng trong thuật giải tạo chữ ký số
C. Cho giá trị băm 160 bit
D. Tất cả đ ều đúng
134. DSA là thuật giải :
A. Lấy dấu tay "PrintingFinger"
B. B . Tạo chữ ký số (DS)
C. Phân phối khoá trước
D. Bảo mật thông điệp
135. Thuật giải MD5 cho ta một giá trị băm có độ dài :
A. 156 bit
B. 256 bit
C. 128 bit
D. 512 bit
136. Trong các cặp khoá sau đây của hệ mật RSA với p=5 ; q=7 , cặp khóa nào có khả năng đúng nhất:
A. (e = 12 , d =11) ;
B. (e = 4 , d =11)
C. ( e = 7 , d =23)
D. ( e = 3 , d =18)
137. Thuật giải Difie Hellman dùng để :
A. Bảo mật thông điệp

B. Xác thực thông điệp
C. Phân phối khoá trước cho hệ mật đối xứng
D. Lấy chữ ký số
138. MAC là một từ cấu tạo bằng những chữ đầu của một nhóm nào liên quan đến mật mã ?
A. Kiểm soát truy cập phương tiện (Media access control)
B. Kiểm soát truy cập bắt buộc (Mandatory access control)
C. Mã xác thực thông điệp (Message authentication code)
D. Các ủy ban đa tư vấn (Multiple advisory committees)
139. Nội dung nào sau đây không cần sử dụng mật mã ?
A. Bảo mật
B. Xác thực
C. Toàn vẹn
D. Truy cập
140. PKC được thực hiện bằng cách sử dụng các chức năng nào ?
A. Chuyển giao các khóa công khai an toàn
B. Chuyển giao các khóa cá nhân an toàn
C. Bảo mật dữ liệu ở hai đầu mút
D. Sử dụng hai khóa khác nhau để mã hóa và giải mã
141. Khái niệm nào sau đây được sử dụng để mô tả sự không thể chối từ của người gửi khi gửi thông điệp ?
A. Toàn vẹn
B. Tính không chối từ ( non-repudiation)
C. Xác thực
D. Bảo mật
142. Khái niệm nào sau đây được dùng để xác định chuẩn thực thi các hệ thống mã hóa diện rộng?
A. PKE
B. PKI
C. Đối xứng
D. Không đối xứng
143. Tổ chức chính cấp phát chứng chỉ được gọi là :
A. CA
B. RA
C. LRA
D. CRL
144. Hầu hết định dạng chứng chỉ công cộng được sử dụng trong môi trường PKI là gì ?
A. X.509
B. X.508
C. PKE

D. RSA
145. Quy trình mã hoá nào sử dụng cùng một khoá mã ở cả hai phía của một phiên làm việc ?
A. Symmetrical
B. Asymmetrical
C. PKCS
D. Split key
146. PKCS sử dụng cặp khoá nào để mã hoá?
A. Symmetric
B. Public/private
C. Asymmetric/symmetric
D. Private/private
147. Giao thức nào sau đây tương tự như SSL và được đề nghị sử dụng bổ sung vào các giao thức bảo mật ?
A. TLS
B. SSH
C. RSH
D. X.509
148. Vấn đề gì nảy sinh khi sử dụng qui trình sinh khóa mã tập trung ?
A. Bảo mật mạng
B. Truyền khóa
C. Thu hồi chứng chỉ
D. Bảo mật khóa cá nhân
149. Giao thức nào sau đây cung cấp dịch vụ bảo mật cho các phiên làm việc trên thiết bị đầu cuối của hệ thống UNIX từ xa ?
A. SSL
B. TLS
C. SSH
D. PKI
150. Dịch vụ nào sau đây là một dịch vụ đơn hay một máy phục vụ để lưu trữ, phân phối, và quản lý các khóa phiên mật mã ?
A. KDC
B. KEA
C. PKI
D. PKCS
151. Bạn có một fille dữ liệu trên đĩa cứng , phương pháp nào theo bạn là tốt nhất để bảo mật dữ liệu đó
A. RSA
B. DES
C. DSA
D. SHA

152. Thuật giải SHA-1 dùng để :
A. Tạo khoá đối xứng
B. Tạo chữ ký số
C. Tạo một giá trị băm có độ dài cố định 160 bit
D. Tạo một giá trị băm có độ dài cố định 256 bit
153. Thuật giải MD5 dùng để :
A. Bảo mật một thông điệp
B. Xác thực một thông điệp
C. Phân phối khoá mật mã
D. Kiểm tra tính toàn vẹn dữ liệu
154. Trong DES mỗi hàm chọn Si được dùng để :
A. Biến đổi khối dữ liệu mã 48 bit thành 32 bit
B. Biến đổi khối dữ liệu mã 6 bít thành 4 bít
C. Biến đổi khối dữ liệu mã 16 bít thành 4 bít
D. Biến đổi khối dữ liệu mã 32 bít thành 4 bít
155. Trong hệ mã công khai RSA , để tạo một chữ ký điện tử của văn bản M ta dùng :
A. S = E( ek ,M)
B. S = D( dk ,M)
C. S = D(ek,M)
D. S = E ( dk ,M)
156. Trong hệ mã công khai RSA , để chứng thực chữ ký điện tử S của văn bản M ta dùng :
A. M = E( ek , S)
B. M = D( dk ,S)
C. M = D(ek , S)
D. M = E (dk ,S)
157. Điều nào sau đây là điểm yếu của IP ?
A. Mã nguồn độc hại
B. Giả mạo IP
C. Tấn công dạng "Man in the middle"
D. Tấn công chuyển tiếp
158. Qui trình xác định topology của mạng được gọi là gì ?
A. In dấu chân
B. Thiết bị làm nhiễu
C. Quét mạng
D. Liệt kê
159. Qui trình xác định vị trí và các thông tin mạng được gọi là gì ?
A. In dấu chân
B. Quét
C. Thiết bị làm nhiễu
D. Liệt kê

160. Qui trình chiếm quyền truy cập đến tài nguyên mạng (đặc biệt như là các tập tin user và nhóm) được gọi là gì ?
A. In dấu chân
B. Quét
C. Thiết bị làm nhiễu
D. Liệt kê
161. Qui trình phá vỡ một phiên làm việc IM được gọi là gì ?
A. Thiết bị làm nhiễu
B. Truyền rộng rãi
C. Phản ứng với rắc rối
D. Khảo sát định vị
162. Bạn mới nhận cuộc gọi từ một user IM trong văn phòng mà user này đang ghé thăm một website quảng cáo. User này đang phàn nàn rằng hệ thống của anh ta không phản ứng và hàng triệu trang web đang mở trên màn hình của anh ta. Loại tấn công này là gì ?
A. DoS
B. Mã nguồn độc hại
C. Giả mạo IP
D. Khảo sát định vị
163. Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng là:
A. Sử dụng các phần cứng hệ thống và mạng đắt tiền
B. Sử dụng tường lửa và các phần mềm quét virus
C. Sử dụng các hệ thống ngăn chặn và phát hiện tấn công, đột nhập
D. Sử dụng nhiều lớp bảo vệ có chiều sâu
164. Đâu là một phương pháp mã hóa:
A. Thay thế
B. Đổi chỗ/hoán vị
C. Vernam
D. Tất cả các phương pháp trên
165. Giao thức bảo mật SSL đảm bảo tính bí mật, toàn vẹn và xác thực thông điệp bằng các kỹ thuật nào sau đây:
A. Mã hóa khóa bí mật và hàm băm có khóa MAC
B. Mã hóa khóa bí mật và chữ ký số
C. Mã hóa khóa bí mật và mã hóa khóa công khai
D. Mã hóa khóa bí mật và hàm băm không khóa MDC
166. Các hệ mã hóa khóa công khai sử dụng một cặp khóa: public key và private key. Các yêu cầu đối với public key và private key là:
A. Cả public key và private key đều cần giữ bí mật
B. Có thể công khai public key và cần giữ bí mật private key
C. Có thể công khai private key và cần giữ bí mật public key
D. Có thể công khai public key nhưng phải đảm bảo tính xác thực và cần giữ bí mật

private key
167. Sâu SQL Slammer là sâu tấn công các hệ thống mạng lợi dụng lỗ hổng tràn bộ đệm ở:
A. Máy chủ CSDL Microsoft SQL Server 2008
B. Hệ điều hành Microsoft Windows 2003
C. Máy chủ CSDL Microsoft SQL Server 2005
D. Máy chủ CSDL Microsoft SQL Server 2000
168. Kích thước khóa có thể của hệ mã hóa AES là:
A. 128, 160 và 192 bít
B. 64, 128 và 192 bít
C. 128, 256 và 512 bít
D. 128, 256 và 384 bít
169. Các lỗ hổng tồn tại phổ biến trong trong hệ điều hành và các phần mềm ứng dụng là:
A. Lỗi tràn bộ đệm và lỗi không kiểm tra đầu vào
B. Lỗi tràn bộ đệm và cấu hình
C. Lỗi cài đặt và quản trị
D. Lỗi cài đặt và cấu hình
170. Phát biểu nào sau đây mô tả đúng nhất về kỹ thuật tấn công Smurf:
A. Giả mạo địa chỉ IP nguồn trong gói tin ICMP là địa chỉ máy đích và chúng gửi đến tất cả các máy trong mạng
B. Giả mạo địa chỉ IP nguồn trong gói tin ICMP là địa chỉ máy đích và chúng gửi đến địa chỉ quảng bá của mạng
C. Giả mạo địa chỉ IP nguồn trong gói tin ICMP là địa chỉ quảng bá và chúng gửi đến máy đích
D. Tạo và gửi rất nhiều gói tin ICMP giả mạo có kích thước lớn đến máy đích
171. An toàn hệ thống thông tin là việc đảm bảo các thuộc tính an ninh, an toàn nào của hệ thống thông tin:
A. Bí mật, xác thực và điều khiển
B. Bí mật, toàn vẹn và không chối bỏ
C. Bí mật, xác thực và không chối bỏ
D. Bí mật, toàn vẹn và sẵn dùng
172. Trong quá trình thiết lập một phiên kết nối TCP (TCP three-way handshake) thứ tự các gói tin được gửi đi như thế nào?
A. SYN, URG, ACK
B. SYN, ACK, SYN-ACK
C. SYN, SYN-ACK, ACK
D. FIN, FIN-ACK, ACK
173. Khi một website tồn tại lỗ hổng SQL Injection, nguy cơ cao nhất có thể xảy ra là:
A. Chiếm quyền điều khiển hệ thống

B. Chèn, xóa hoặc sửa đổi dữ liệu
C. Đánh cắp các thông tin trong CSDL
D. Tấn công thay đổi hình ảnh giao diện
174. Đặc trưng cơ bản khác biệt của worm với virus là:
A. Có khả năng phá hoại lớn hơn so với virus
B. Có khả năng tự lây lan mà không cần vật chủ hoặc tác nhân
C. Có khả năng lây lan nhanh chóng bằng nhiều phương pháp khác nhau
D. Có khả năng chiếm quyền điều khiển hệ thống
175. Sự khác biệt giữa hệ chữ ký số RSA và DSA là:
A. RSA an toàn hơn DSA
B. DSA an toàn hơn RSA
C. DSA có chi phí tính toán thấp hơn RSA
D. Giải thuật DSA đơn giản hơn giải thuật RSA
176. Kích thước khóa hiệu dụng của hệ mã hóa DES là:
A. 64 bít
B. 48 bít
C. 56 bít
D. 128 bít
177. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state. Kích thước của state là:
A. 160 bít
B. 170 bít
C. 150 bít
D. 180 bít
178. Sự khác biệt cơ bản giữa tấn công DoS và tấn công DDoS là:
A. DoS chỉ gây ngập lụt đường truyền
B. DDoS chỉ làm cạn kiệt tài nguyên máy chủ
C. Số hosts tham gia tấn công
D. Cơ chế tấn công DDoS phức tạp hơn
179. Số lượng vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã trong hệ mã hóa AES khóa 128 bít là:
A. 14
B. 10
C. 16
D. 12
180. Loại tấn công nào sau đây cung cấp cho tin tặc nhưng thông tin hữu ích về các dịch vụ đang chạy trên hệ thống?
A. Vulnerability Scan
B. Session Hijacking
C. Port Scan
D. IP sweep

181. Bước MixColumns (trộn cột) trong vòng lặp chuyển đổi trong hệ mã hóa AES thực hiện việc:
A. Trộn hai cột kềnhau của ma trận state
B. Mỗi cột của ma trận state được nhân với một đa thức
C. Trộn các cột tương ứng của ma trận state với khóa
D. Trộn các dòng tương ứng của ma trận state với khóa
182. Tấn công dựa trên từ điển là:
A. Sử dụng từ điển để tấn công đánh cắp mật khẩu của người dùng
B. Tấn công vào thói quen sử dụng các từ đơn giản có trong từ điển làm mật khẩu
C. Nghe trộm để đánh cắp mật khẩu
D. Thử tất cả các khả năng kiểu vét cạn để tìm mật khẩu của người dùng
183. Các phần mềm độc hại nào sau đây có khả năng tự nhân bản:
A. Virus, worm, adware
B. Virus, backdoor, worm
C. Virus, worm, zombie
D. Virus, trojan horse, worm
184. SET là giao thực bảo mật dùng trong các giao dịch điện tử. Với SET, những bên nào tham gia giao dịch phải có chứng chỉ số:
A. Tất cả các bên
B. Khách hàng
C. Cổng giao dịch
D. Người bán
185. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập MAC:
A. MAC cấp quyền truy cập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
B. MAC là cơ chế điều khiển truy cập được sử dụng rộng rãi nhất
C. MAC cho phép người tạo ra đối tượng có thể cấp quyền truy cập cho người dùng khác
D. MAC quản lý quyền truy cập chặt chẽ hơn các cơ chế khác
186. Phát biểu nào sau đây đúng với kỹ thuật mã hóa khóa bí mật:
A. Mã hóa khóa bí mật an toàn hơn mã hóa khóa công khai
B. Mã hóa khóa bí mật chỉ hoạt động theo chế độ mã hóa khối
C. Mã hóa khóa bí mật sử dụng một khóa mã (key) cho cả quá trình mã hóa và giải mã
D. Mã hóa khóa bí mật có thuật toán đơn giản hơn mã hóa khóa công khai
187. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập RBAC:
A. RBAC cho phép người tạo ra đối tượng có thể cấp quyền truy cập cho người dùng khác
B. RBAC cấp quyền truy cập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
C. RBAC cấp quyền truy cập dựa trên vai trò của người dùng trong tổ chức

D. RBAC là cơ chế điều khiển truy cập được sử dụng rộng rãi nhất
188. An toàn thông tin An toàn thông tin (Information Security) là:
A. Việc đảm bảo an toàn cho hệ thống máy tính.
B. Việc phòng chống tấn công, đột nhập vào hệ thống máy tính và mạng.
C. Việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép.
D. Việc đảm bảo an toàn cho hệ thống mạng.
189. Nguyên nhân chính của lỗ hổng an ninh cho phép tấn công thực hiện mã từ xa là:
A. Lỗi thiết kế phần mềm
B. Lỗi quản trị hệ thống
C. Lỗi lập trình phần mềm
D. Lỗi tích hợp hệ thống
190. Danh sách điều khiển truy cập ACL thực hiện việc cấp quyền truy cập đến các đối tượng cho người dùng bằng cách:
A. Các quyền truy cập vào đối tượng cho mỗi người dùng được quản lý riêng rẽ
B. Mỗi người dùng được gán một danh sách các đối tượng kèm theo quyền truy cập
C. Các quyền truy cập vào đối tượng cho mỗi người dùng được quản lý trong một ma trận
D. Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy cập
191. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập DAC:
A. DAC cho phép người tạo ra đối tượng có thể cấp quyền truy cập cho người dùng khác
B. DAC cấp quyền truy cập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
C. DAC quản lý quyền truy cập chặt chẽ hơn các cơ chế khác
D. DAC là cơ chế điều khiển truy cập được sử dụng rộng rãi nhất
192. Loại tấn công nào sau đây chiếm quyền truy cập đến tài nguyên lợi dụng cơ chế điều khiển truy cập DAC?
A. Phishing
B. Trojan horse
C. Spoofing
D. Man in the middle
193. Phương pháp xác thực nào dưới đây cung cấp khả năng xác thực có độ an toàn cao nhất?
A. Sử dụng mật khẩu
B. Sử dụng Smartcard
C. Sử dụng chứng chỉ số
D. Sử dụng vân tay
194. Macro virus là virus lây nhiễm trong:
A. Các file tài liệu dạng PDF
B. Các file tài liệu của bộ chương trình Open Office

C. Các file ảnh dạng JPG
D. Các file tài liệu của bộ chương trình MS Office
195. Phát biểu nào sau đây đúng với tường lửa
A. Tường lửa không thể ngăn chặn các tấn công hướng dữ liệu
B. Tường lửa có thể ngăn chặn mọi loại tấn công, đột nhập
C. Tường lửa có thể ngăn chặn mọi virus và phần mềm độc hại
D. Tường lửa có thể ngăn chặn các loại thư rác
196. Trong quá trình xử lý dữ liệu tạo chuỗi băm, số lượng vòng xử lý của SHA1 là:
A. 60
B. 70
C. 80
D. 90
197. Một trong các biện pháp hiệu quả phòng chống tấn công SQL Injection là:
A. Luôn kiểm tra và cập nhật các bản vá an ninh cho hệ điều hành và các phần mềm ứng dụng
B. Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy
C. Cấu hình máy chủ CSDL không cho thực thi lệnh từ xa
D. Không cho phép người dùng nhập mã vào các form.
198. Trong hệ thống Kerberos gồm 3 thực thể: client A, máy chủ Kerberos T, máy chủ ứng dụng B, mục đích của hệ thống là để:
A. T hỗ trợ A xác thực thông tin nhận dạng với B, kèm theo thiết lập khóa
B. T xác thực B
C. T xác thực A và B
D. T xác thực A
199. SSL sử dụng giao thực SSL Handshake để khởi tạo phiên làm việc. SSL Handshake thực hiện việc xác thực thực thể dựa trên:
A. Chữ ký số
B. Chứng chỉ số
C. Mã hóa khóa công khai
D. Mã hóa khóa bí mật
200. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là:
A. MDC an toàn hơn MAC
B. MAC an toàn hơn MDC
C. MDC có khả năng chống đụng độ cao hơn MAC
D. MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa
201. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây:
A. Xác thực, đăng nhập và kiểm toán (auditing)
B. Xác thực, đăng nhập và trao quyền
C. Xác thực, trao quyền và kiểm toán (auditing)

D. Xác thực, trao quyền và quản trị
202. Ưu điểm của kỹ thuật mã hóa khóa công khai so với mã hóa khóa bí mật là:
A. Có độ an toàn cao hơn
B. Trao đổi khóa dễ dàng hơn
C. Chi phí tính toán thấp hơn
D. Quản lý dễ dàng hơn
203. Độ an toàn của hệ mã hóa RSA dựa trên:
A. Khóa có kích thước lớn
B. Giải thuật rất phức tạp
C. Chi phí tính toán lớn
D. Tính khó của việc phân tích số nguyên lớn
204. Trong hệ mã hóa RSA, quan hệ toán học giữa khóa bí mật d và khóa công khai e được gọi là:
A. d và e là 2 số nguyên tố cùng nhau
B. d là modulo nghịch đảo của e
C. d là modulo của e
D. d và e không có quan hệ với nhau
205. Trong hệ thống phân phối khóa sử dụng KTC gồm có n thực thể (không tính KTC), số lượng khóa dài hạn mỗi thực thể và KTC phải lưu là:
A. Mỗi thực thể phải lưu 1 khóa, KTC phải lưu n2 khóa
B. Mỗi thực thể phải lưu 1 khóa, KTC phải lưu n khóa
C. Mỗi thực thể phải lưu n-1 khóa, KTC phải lưu n khóa
D. Mỗi thực thể phải lưu 1 khóa, KTC phải lưu 1 khóa
206. Số lượng các khóa phụ (subkey) cần được tạo ra từ khóa chính trong giải thuật DES là:
A. 18
B. 16
C. 14
D. 12
207. Các thuộc tính cơ bản của chứng chỉ số (Digital certificate) gồm:
A. Số nhận dạng, khóa công khai của chủ thể, thông tin định danh chủ thể
B. Khóa công khai của chủ thể, thông tin định danh chủ thể, thuật toán chữ ký sử dụng
C. Số nhận dạng, khóa công khai của chủ thể, chữ ký của nhà cung cấp CA
D. Khóa công khai của chủ thể, thông tin định danh chủ thể, chữ ký của nhà cung cấp CA
208. Công cụ Vulnerability scanner cho phép tin tặc:
A. Tìm các cổng dịch vụ đang mở trên hệ thống
B. Thu thập các thông tin về các điểm yếu/lỗ hổng đã biết của hệ thống máy tính hoặc mạng
C. Nghe trộm và bắt các gói tin khi chúng được truyền trên mạng

D. Chặn bắt và sửa đổi thông tin
209. Sự khác biệt giữa trung tâm phân phối khóa KDC và trung tâm dịch khóa KTC là:
A. KDC an toàn hơn KTC
B. KTC an toàn hơn KDC
C. KDC sinh khóa tập trung, còn KTC sinh khóa phân tán
D. KDC yêu cầu có một máy chủ tin cậy, còn KTC không yêu cầu có một máy chủ tin cậy
210. Tấn công lợi dụng lỗi tràn bộ đệm có thể giúp tin tặc chèn và thực hiện mã độc trên hệ thống nạn nhân thông qua cơ chế nào sau đây:
A. Chèn mã độc vào thay thế mã trong chương trình có lỗi tràn bộ đệm
B. Tất cả các đáp án trên đều đúng
C. Chèn mã độc vào bộ đệm và lợi dụng cơ chế trở về từ chương trình con để thực hiện mã độc đã chèn
D. Chèn mã độc vào bộ đệm và lợi dụng cơ chế gọi thực hiện chương trình con để thực hiện mã độc đã chèn
211. Phát biểu nào sau đây về chữ ký số là chính xác:
A. Chữ ký số được tạo ra bằng cách mã hóa thông điệp sử dụng khóa riêng của chủ thể
B. Chữ ký số được sử dụng để đảm bảo tính bí mật và toàn vẹn thông điệp
C. Chữ ký số được sử dụng để đảm bảo tính bí mật, toàn vẹn và xác thực thông điệp
D. Chữ ký số là một chuỗi dữ liệu liên kết với một thông điệp và thực thể tạo ra thông điệp
212. Số lượng thao tác trong mỗi vòng xử lý của MD5 là:
A. 12
B. 16
C. 14
D. 18
213. Lỗ hổng an ninh trong một hệ thống là:
A. Bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
B. Các điểm yếu trong hệ điều hành
C. Tất cả điểm yếu hoặc khiếm khuyết trong hệ thống
D. Các điểm yếu trong các phần mềm ứng dụng
214. Hai lĩnh vực chính của an toàn thông tin là:
A. Mật mã và An ninh mạng
B. An toàn công nghệ thông tin và An ninh mạng
C. An ninh máy tính và An ninh mạng
D. An toàn công nghệ thông tin và Đảm bảo thông tin
215. Các hệ điều hành Microsoft Windows và Linux sử dụng các mô hình điều khiển truy cập nào dưới đây?
A. DAC và Role-BAC

B. DAC và MAC
C. MAC và Role-BAC
D. MAC và Rule-BAC
216. SSL sử dụng giao thực SSL Handshake để khởi tạo phiên làm việc. SSL Handshake thực hiện việc trao đổi các khóa phiên dùng cho phiên làm việc dựa trên:
A. Chữ ký số
B. Chứng chỉ số
C. Mã hóa khóa công khai
D. Mã hóa khóa bí mật
217. Tấn công bằng mã độc bao gồm các dạng tấn công:
A. Cả A và B
B. Cài đặt và thực hiện các phần mềm độc hại trên hệ thống nạn nhân
C. Lợi dụng các lỗ hổng an ninh để đánh cắp thông tin nhạy cảm
D. Lợi dụng các lỗ hổng an ninh để chèn và thực hiện mã độc trên hệ thống nạn nhân
218. Tấn công Phishing là dạng tấn công vào:
A. Người quản trị và người dùng thông thường
B. Hệ điều hành và các ứng dụng
C. Các hệ thống mạng
D. Các phần mềm máy chủ
219. Điểm khác nhau chính giữa các hệ thống ngăn chặn đột nhập (IPS) và phát hiện đột nhập (IDS) là:
A. IPS có khả năng phát hiện và ngăn chặn tấn công tốt hơn IDS
B. IDS có khả năng phát hiện và ngăn chặn tấn công tốt hơn IPS
C. IPS có khả năng chủ động ngăn chặn tấn công so với IDS
D. IPS có chi phí lớn hơn IDS
220. Gửi một gói tin ICMP có kích thước lớn hơn 64Kb là một ví dụ của kiểu tấn công nào sau đây?
A. Buffer overflow
B. Syn flood
C. Teardrop
D. Ping of Death
221. Chữ ký số (dùng riêng) thường được sử dụng để đảm bảo thuộc tính nào sau đây của thông điệp truyền:
A. Tính bí mật
B. Tính toàn vẹn
C. Tính xác thực
D. Tính không chối bỏ
222. Tấn công DoS là dạng tấn công cho phép tin tặc:
A. Gây ngắt quãng dịch vụ cung cấp cho người dùng bình thường
B. Đánh cắp dữ liệu trên máy chủ
C. Đánh cắp dữ liệu trên máy khách

D. Sửa đổi dữ liệu trong CSDL
223. 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
224. 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
225. 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
226. Cơ chế bảo mật SSL hoạt động trên tầng
A. Network, Transport
B. Network, Session
C. Application, Session
D. Tất cả đều sai
227. 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
228. 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
229. Công cụ/cơ chế bảo mật cho mạng không dây là
A. SSL
B. TSL
C. Giao thức PGP
D. WEP
230. Giao thức SSL và TSL hoạt động ở tầng nào của mô hình OSI
A. Network
B. Sesion
C. Transport

D. Từ t`ầng Transport trở lên
231. 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 Platform Window
232. 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 đ`ều đúng
233. 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
234. Các dạng sau đây, dạng nào là của virus
A. stealth, cư trú bộ nhớ, macro, đa hình, file
B. stealth, cư trú bộ nhớ, macro, lưỡng tính, file
C. virus ký sinh, file, boot sector, stealth, cư trú bộ nhớ, macro
D. virus ký sinh, cư trú bộ nhớ, boot sector, Stealth, đa hình, macro
235. 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
236. Các giao thức bảo mật trên Internet như SSL, TLS và SSH hoạt động ở t`ầng nào trên mô hình OSI
A. T`ầng Network
B. T`ầng Transport
C. Từ t`ầng Transport trở lên đến t`ầng 7
D. T`ầng Session
237. 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.
238. Các lỗ hổng bảo mật trên hệ thống là do
A. Dịch vụ cung cấp
B. Bản thân hệ đi`ều hành

C. Con người tạo ra
D. Tất cả đều đúng
239. 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
240. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên ( session) của mô hình OSI
A. Packet filtering firewall(lop mang)
B. Circuit level firewall(lop phien)
C. Application level firewall(lop ung dung)
D. Stateful multilayer inspection firewall
241. 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
242. 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.
243. 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
244. 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

245. 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
246. 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
247. 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
248. 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
249. 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. d.Không có bước nào ở trên là đúng
250. 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. SHATR
251. Để thực hiện tấn công bằng Trojan, kẻ tấn công chỉ c`ần
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 đ`ồng thời 2 file, một file vận hành trên máy nạn nhân, file còn lại hoạt động đi`ều khiển trên máy kẻ tấn công.
D. Không có đi`ều nào đúng.
252. Giao thức bảo mật IPSec hoạt động ở t`ầng
A. Chỉ ở t`ầng transport ở mô hình OSI
B. Từ t`ầng 4 tới t`ầng 7 ở mô hình OSI
C. Network Layer ở mô hình OSI
D. Tất cả đ`ều sai
253. Cho biết phát biểu sau đây phát biểu nào là đúng nhất v`êregistry
A. Regỉstry là một cơ sở dữ liệu dùng để lưu trữ thông tin v`ênhững sự thay đổi, những lựa chọn, những thiết lập từ người sử dụng Windows.
B. Regỉstry là một ph`ần m`ềm tiện ích hỗ trợ cho người dùng thay đổii cấu hình Window khi c`ần thiết
C. Regỉstry là một thành ph`ần của hệ đi`ều hành Window
D. Tất cả đ`ều đúng
254. Có bao nhiêu kiểu dữ liệu trong Registry
A. 5
B. 4
C. 6
D. 7
255. 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
256. 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 đ`ều sai
257. 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
258. 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
259. 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
260. Thuật tóan thực hiện trong cơ chế bảo mật IP (IPSec) ở Window sử dụng là
A. MD5 và SHA1
B. Kerberos và DES
C. DES hoặc 3DES (triple DES).
D. Tất cả đều sai
261. 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
262. 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
263. Quy trình crack một sản phẩm phần mềm đơn giản gồm mấy bước
A. 3
B. 4
C. 5
D. 3 hoặc 4
264. 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
265. 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
266. 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
267. 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
268. 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
269. 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
270. 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
271. 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

272. 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
273. Mã 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
274. 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
275. 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
276. 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
277. 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
278. Sử dụng nhiêu bit với DES để có hiệu quả?
A. 56
B. 64
C. 32
D. 16
279. 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
280. Đối với Firewall 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
281. 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
282. DES là viết tắt của từ nào ?
A. Data encryption system
B. Data encryption standard
C. Data encoding standard
D. Data encryption signature
283. 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
284. Giai đoạn đầu của hacking là gì?
A. Duy trì truy cập
B. Gaining truy cập
C. Trinh sát
D. Dò tìm (Scanning)
285. 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
286. 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
287. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì?

A. Scanning
B. Enumeration
C. System hacking
D. Active information gathering
288. 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
289. 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.
290. FTP sử dụng cổng gì ?
A. 21
B. 25
C. 23
D. 80
291. Cổng nào được HTTPS sử dụng?
A. 443
B. 80
C. 53
D. 21
292. 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
293. 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
294. 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
295. 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
296. 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
297. 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