**NGÂN HÀNG CÂU HỎI TRẮC NGHIỆM**

*(Phục vụ sát hạch năng lực công chức viên chức làm nhiệm vụ đảm bảo an toàn thông tin tỉnh Lào Cai)*

1. Theo Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước. Nội dung quy định về “Điều kiện bảo đảm thực hiện nhiệm vụ an toàn thông tin”?
2. Cán bộ, công chức, viên chức phải nắm vững các quy định của pháp luật và nội quy của cơ quan về an toàn thông tin.
3. Cán bộ kỹ thuật về an toàn thông tin phải được tuyển chọn, đào tạo, huấn luyện, thường xuyên bồi dưỡng nghiệp vụ phù hợp với nhiệm vụ được giao và được tạo điều kiện làm việc phù hợp.
4. Hạ tầng kỹ thuật phải được định kỳ kiểm tra, đánh giá hoặc kiểm định về mặt an toàn thông tin phù hợp các tiêu chuẩn, quy chuẩn kỹ thuật quy định.
5. Tất cả các phương án trên.
6. Theo Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước. Nội dung quy định về “Trách nhiệm giải quyết và khắc phục sự cố an toàn thông tin” của cơ quan nhà nước có hạ tầng kỹ thuật bị sự cố?
7. Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo cho cơ quan cấp trên quản lý trực tiếp.
8. Tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố và thực hiện theo đúng hướng dẫn.
9. Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết cho cơ quan cấp trên quản lý trực tiếp.
10. Tất cả các phương án trên.
11. Theo Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước. Nội dung quy định về “Việc bảo đảm an toàn thông tin”?
12. Cơ quan nhà nước phải xây dựng nội quy bảo đảm an toàn thông tin.
13. Khuyến khích Cơ quan nhà nước xây dựng nội quy bảo đảm an toàn thông tin.
14. Cả phương án a và b đều sai.
15. Cả phương án a và b đều đúng.
16. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định việc áp dụng quy trình bảo đảm an toàn dữ liệu bao gồm?
17. Lưu trữ dự phòng. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã.
18. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước; giám sát các khâu tạo lập, xử lý và hủy bỏ dữ liệu.
19. Tất cả các phương án trên.
20. Cả phương án a và b đều sai.
21. Luật CNTT số 67/2006/QH11, ngày 12/07/2006, quy định về “Bảo đảm an toàn, bí mật thông tin”, tổ chức, cá nhân không được thực hiện một trong những hành vi sau đây?
22. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng; cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin;
23. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng.
24. Thông báo cho cơ quan quản lý Nhà nước chuyên trách CNTT về nguy cơ mất an toàn thông tin.
25. Phương án a và b.
26. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nội dung quản lý nhà nước về công nghệ thông tin, nội dung nào sau đây là sai?
27. Xây dựng, tổ chức thực hiện chiến lược, quy hoạch, kế hoạch, chính sách ứng dụng và phát triển công nghệ thông tin.
28. Quản lý an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.
29. Quản lý thống kê về công nghệ thông tin.
30. Cả 3 nội dung trên đều sai.
31. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Chính sách của Nhà nước về ứng dụng và phát triển công nghệ thông tin, nội dung nào sau đây là đúng?
32. Ưu tiên ứng dụng và phát triển công nghệ thông tin trong chiến lược phát triển kinh tế - xã hội và sự nghiệp công nghiệp hóa, hiện đại hóa đất nước.
33. Tạo điều kiện để tổ chức, cá nhân hoạt động ứng dụng và phát triển công nghệ thông tin đáp ứng yêu cầu phát triển kinh tế - xã hội, đối ngoại, quốc phòng, an ninh; thúc đẩy công nghiệp công nghệ thông tin phát triển thành ngành kinh tế trọng điểm, đáp ứng nhu cầu thị trường nội địa và xuất khẩu.
34. 4. Ưu tiên dành một khoản ngân sách nhà nước để ứng dụng công nghệ thông tin trong một số lĩnh vực thiết yếu, tạo lập nền công nghiệp công nghệ thông tin và phát triển nguồn nhân lực công nghệ thông tin.
35. Cả 3 nội dung trên đều đúng.
36. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Chính sách của Nhà nước về ứng dụng và phát triển công nghệ thông tin, nội dung nào sau đây là đúng?
37. Tạo điều kiện thuận lợi để phát triển cơ sở hạ tầng thông tin quốc gia. Khuyến khích đầu tư cho lĩnh vực công nghệ thông tin.
38. Có chính sách ưu đãi để tổ chức, cá nhân có hoạt động ứng dụng và phát triển công nghệ thông tin đối với nông nghiệp; nông thôn, vùng sâu, vùng xa, biên giới, hải đảo; người dân tộc thiểu số, người tàn tật, người có hoàn cảnh khó khăn.
39. Bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân ứng dụng và phát triển công nghệ thông tin. Tăng cường giao lưu và hợp tác quốc tế; khuyến khích hợp tác với tổ chức, cá nhân Việt Nam ở nước ngoài trong lĩnh vực công nghệ thông tin.
40. Cả 3 nội dung trên đều đúng.
41. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định về Bảo đảm truy nhập thông tin và khai thác dịch vụ hành chính công, nội dung nào sau đây là đúng?
42. Ủy ban nhân dân cấp tỉnh có chính sách khuyến khích các tổ chức, cá nhân triển khai rộng khắp các điểm truy nhập Internet công cộng; đồng thời tăng cường hướng dẫn phương pháp truy nhập và sử dụng thông tin, dịch vụ hành chính công trên môi trường mạng theo đúng quy định của pháp luật.
43. Áp dụng các mức bảo vệ phù hợp theo đúng phân loại thông tin.
44. Quy định rõ các điều kiện duy trì dữ liệu bao gồm cả việc thay đổi, hủy bỏ dữ liệu. Thường xuyên đánh giá các điều kiện bảo đảm an toàn cho dữ liệu.
45. Cơ sở dữ liệu của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh được xây dựng và tổ chức phù hợp với cơ sở dữ liệu quốc gia.
46. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định về Xây dựng cơ sở dữ liệu quốc gia, nội dung nào sau đây là đúng?
47. Cơ sở dữ liệu quốc gia là tập hợp thông tin của một hoặc một số lĩnh vực kinh tế - xã hội được xây dựng, cập nhật và duy trì đáp ứng yêu cầu truy nhập và sử dụng thông tin của các ngành kinh tế và phục vụ lợi ích xã hội.
48. Bộ Bưu chính, Viễn thông chủ trì, phối hợp với các cơ quan liên quan xây dựng, trình Thủ tướng Chính phủ ban hành danh mục cơ sở dữ liệu quốc gia và quy định trách nhiệm của các cơ quan nhà nước trong việc xây dựng cơ sở dữ liệu quốc gia theo quy định tại khoản 3 Điều này.
49. Cơ quan nhà nước được giao nhiệm vụ chủ trì xây dựng và duy trì cơ sở dữ liệu quốc gia chịu trách nhiệm ban hành Quy chế xây dựng, quản lý, khai thác, bảo vệ và duy trì cơ sở dữ liệu quốc gia đó.
50. Cả 3 nội dung trên đều đúng.
51. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định về Xây dựng cơ sở dữ liệu của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh*,* nội dung nào sau đây là đúng?
52. Cơ sở dữ liệu của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh là tập hợp thông tin được xây dựng, cập nhật và duy trì đáp ứng yêu cầu truy nhập, sử dụng thông tin của mình và phục vụ lợi ích xã hội.
53. Kinh phí xây dựng và duy trì cơ sở dữ liệu của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh được tổng hợp vào dự toán chi ngân sách của ngành hoặc địa phương đó.
54. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh quy định danh mục cơ sở dữ liệu; xây dựng, cập nhật và duy trì cơ sở dữ liệu; ban hành Quy chế xây dựng, quản lý, khai thác, bảo vệ và duy trì cơ sở dữ liệu của mình.
55. Cả 3 nội dung trên đều đúng.
56. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Thông báo về việc tạm ngừng cung cấp thông tin, dịch vụ trên môi trường mạng,nội dung nào sau đây là đúng?
57. Thông báo công khai bằng hình thức phù hợp, trừ trường hợp bất khả kháng, và tiến hành các biện pháp khắc phục sự cố ngay sau khi hệ thống thông tin của cơ quan nhà nước bị lỗi trong quá trình hoạt động làm ảnh hưởng nghiêm trọng hoặc gây ngừng cung cấp thông tin và dịch vụ của cơ quan đó trên môi trường mạng;
58. Cơ quan nhà nước không có trách nhiệm chuẩn bị và triển khai các phương án sử dụng cơ sở hạ tầng thông tin dự phòng để tiếp tục cung cấp thông tin và dịch vụ cần thiết nhất ở mức độ phù hợp trong thời gian tạm ngừng cung cấp thông tin, dịch vụ trên môi trường mạng.
59. Nội dung thông báo không phải nêu rõ khoảng thời gian dự kiến phục hồi các hoạt động cung cấp thông tin và dịch vụ trên môi trường mạng của cơ quan đó.
60. Cả 3 nội dung trên đều đúng.
61. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Kết nối cơ sở hạ tầng thông tin của cơ quan nhà nước với mạng Internet,nội dung nào sau đây là đúng?
62. Cơ quan nhà nước có trách nhiệm kết nối hạ tầng kỹ thuật của mình với mạng Internet để cung cấp thông tin và dịch vụ hành chính công theo chức năng, nhiệm vụ của mình.
63. Việc kết nối Internet phải bảo đảm an toàn thông tin theo quy định tại Điều 41 Nghị định này và các quy định khác của pháp luật.
64. Tất cả các phương án trên.
65. Cả phương án a và b đều sai.
66. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Trách nhiệm cung cấp, tiếp nhận thông tin trên môi trường mạng,nội dung nào sau đây là đúng?
67. Cơ quan nhà nước không có trách nhiệm cung cấp trên môi trường mạng những thông tin theo quy định.
68. Việc cung cấp thông tin không cần thực hiện theo nguyên tắc tạo điều kiện cho người dân tiếp cận nhanh chóng, dễ dàng, tránh phải cung cấp nhiều lần cùng một nội dung thông tin.
69. Cơ quan nhà nước không phải có trách nhiệm tạo thuận lợi cho các hoạt động trên môi trường mạng.
70. Cơ quan nhà nước, người đứng đầu cơ quan nhà nước, tổ chức, cá nhân thực hiện các quyền và nghĩa vụ khác theo quy định của pháp luật về cung cấp thông tin.
71. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định về Xây dựng thống nhất biểu mẫu điện tử , nội dung nào sau đây là đúng?
72. Biểu mẫu điện tử trong giao dịch giữa các cơ quan nhà nước, tổ chức và cá nhân phải tuân theo các quy định của pháp luật và đáp ứng các yêu cầu
73. Danh sách các biểu mẫu điện tử phải được tổ chức khoa học, phân nhóm hợp lý, cập nhật kịp thời để giúp các tổ chức, cá nhân có thể tìm chính xác các biểu mẫu cần thiết dễ dàng và nhanh chóng trên trang thông tin điện tử của cơ quan đó.
74. Các biểu mẫu điện tử riêng theo đặc thù của từng Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ do cơ quan đó tự quy định theo nguyên tắc chung tại khoản 1 và 2 Điều này.
75. Tất cả các phương án trên.
76. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Trang thông tin điện tử của cơ quan nhà nước, nội dung nào sau đây là đúng?
77. Áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật quy định;
78. Hiển thị thông tin nhanh chóng; Quy định rõ thời hạn tồn tại trực tuyến của từng loại thông tin
79. Có công cụ tìm kiếm thông tin dễ sử dụng và cho kết quả đúng nội dung cần tìm kiếm;
80. Tất cả các phương án trên.
81. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Danh mục dịch vụ hành chính công, nội dung nào sau đây là đúng?
82. Công bố danh mục, lộ trình cung cấp các dịch vụ hành chính công trên môi trường mạng.
83. Hướng dẫn tổ chức, cá nhân tham gia giao dịch với cơ quan nhà nước khi thực hiện các dịch vụ hành chính công trên môi trường mạng.
84. Thực hiện việc tuyên truyền, quảng bá để thu hút người dân tham gia giao dịch với cơ quan nhà nước trên môi trường mạng.
85. Tất cả các phương án trên.
86. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Cán bộ chuyên trách về công nghệ thông tin trong các cơ quan nhà nước được hưởng chế độ ưu đãi về điều kiện làm việc, nội dung nào sau đây là đúng?
87. Ưu đãi về sử dụng cơ sở hạ tầng thông tin và trang thiết bị;
88. Ưu đãi về đào tạo, nâng cao trình độ công nghệ thông tin;
89. Ưu đãi khác phù hợp với quy định của pháp luật.
90. Tất cả các phương án trên.
91. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Biên chế cán bộ chuyên trách về công nghệ thông tin, nội dung nào sau đây là đúng?
92. Cơ quan nhà nước có trách nhiệm bố trí đủ cán bộ chuyên trách về công nghệ thông tin, phù hợp với kế hoạch ứng dụng công nghệ thông tin trong cơ quan mình.
93. Cơ quan nhà nước không có trách nhiệm bố trí đủ cán bộ chuyên trách về công nghệ thông tin, phù hợp với kế hoạch ứng dụng công nghệ thông tin trong cơ quan mình.
94. Khuyến khích các cơ quan nhà nước ban hành quy định ưu đãi về thu nhập cho nhân lực công nghệ thông tin trong cơ quan mình; quy định về tiêu chuẩn, trách nhiệm, quyền lợi, yêu cầu đánh giá mức độ hoàn thành nhiệm vụ của cán bộ, công chức, viên chức đối với việc ứng dụng công nghệ thông tin trong công việc của mình.
95. Tất cả các phương án trên.
96. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Ưu tiên bố trí ngân sách cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là đúng?
97. Đầu tư cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước là đầu tư phát triển.
98. Bộ Kế hoạch và Đầu tư, Bộ Tài chính ưu tiên bố trí ngân sách cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.
99. Hàng năm, cơ quan nhà nước có thẩm quyền cấp đủ kinh phí và đúng thời hạn cho ứng dụng công nghệ thông tin theo kế hoạch được phê duyệt.
100. Tất cả các phương án trên.
101. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Đầu tư cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là đúng?
102. Xây dựng mới, bảo trì, nâng cấp hạ tầng kỹ thuật;
103. Xây dựng mới, mua sắm, bảo trì, nâng cấp phần mềm;
104. Xây dựng, cập nhật, duy trì và sao lưu cơ sở dữ liệu, các hệ thống thông tin quản lý; Tích hợp hệ thống;
105. Tất cả các phương án trên.
106. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Khuyến khích đầu tư ứng dụng công nghệ thông tin, nội dung nào sau đây là đúng?
107. Nhà nước khuyến khích đầu tư ứng dụng công nghệ thông tin từ các nguồn vốn không phải ngân sách nhà nước
108. Cho hoạt động của các cơ quan nhà nước, địa phương ở nông thôn, vùng sâu, vùng xa, miền núi, hải đảo và các vùng khó khăn.
109. Tất cả các phương án trên.
110. Cả phương án a và b đều sai.
111. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Quyền sở hữu trí tuệ đối với giải pháp, phần mềm, cơ sở dữ liệu, nội dung nào sau đây là đúng?
112. Quyền sở hữu trí tuệ, quyền phát triển giải pháp, phần mềm, cơ sở dữ liệu trong các dự án ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải thực hiện theo quy định của pháp luật về sở hữu trí tuệ.
113. Quyền sở hữu trí tuệ, quyền phát triển giải pháp, phần mềm, cơ sở dữ liệu trong các dự án ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước không phải thực hiện theo quy định của pháp luật về sở hữu trí tuệ và được xác định rõ trong hợp đồng.
114. Quyền sở hữu trí tuệ, quyền phát triển giải pháp, phần mềm, cơ sở dữ liệu trong các dự án ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải thực hiện theo quy định của pháp luật về sở hữu trí tuệ và được xác định rõ trong hợp đồng.
115. Quyền sở hữu trí tuệ, quyền phát triển giải pháp, phần mềm, cơ sở dữ liệu trong các dự án ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải thực hiện và được xác định rõ trong hợp đồng.
116. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Đánh giá mức độ ứng dụng công nghệ thông tin, nội dung nào sau đây là đúng?
117. Cơ quan nhà nước ứng dụng công nghệ thông tin định kỳ đánh giá mức độ ứng dụng công nghệ thông tin trong hoạt động của cơ quan mình.
118. Bộ Bưu chính, Viễn thông chịu trách nhiệm hướng dẫn các cơ quan nhà nước thực hiện việc đánh giá mức độ ứng dụng công nghệ thông tin.
119. Tất cả các phương án trên.
120. Cả phương án a và b đều sai.
121. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Giá trị pháp lý của văn bản điện tử, nội dung nào sau đây là đúng?
122. Văn bản điện tử phù hợp với pháp luật về giao dịch điện tử có giá trị pháp lý tương đương với văn bản giấy trong giao dịch giữa các cơ quan nhà nước.
123. Văn bản điện tử gửi đến cơ quan nhà nước không nhất thiết phải sử dụng chữ ký điện tử nếu văn bản đó có thông tin về người gửi*,* bảo đảmtính xácthực về nguồn gốc và sự toàn vẹn của văn bản.
124. Tất cả các phương án trên.
125. Cả phương án a và b đều sai.
126. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Thời điểm gửi, nhận văn bản điện tử, nội dung nào sau đây là đúng?
127. Thời điểm gửi một văn bản điện tử tới cơ quan nhà nước là thời điểm văn bản điện tử này nhập vào hệ thống thông tin nằm ngoài sự kiểm soát của người khởi tạo.
128. Cơ quan nhà nước được Chính phủ giao trách nhiệm có nhiệm vụ xây dựng hệ thống thông tin bảo đảm xác định được thời điểm nhận và gửi văn bản điện tử. Thời điểm nhận là thời điểm văn bản điện tử nhập vào hệ thống thông tin được chỉ định.
129. Tất cả các phương án trên.
130. Cả phương án a và b đều sai.
131. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Tiếp nhận văn bản điện tử và lập hồ sơ lưu trữ, nội dung nào sau đây là đúng?
132. Văn bản điện tử gửi đến cơ quan nhà nước phải được sao lưu trong hệ thống lưu trữ điện tử.
133. Việc sao lưu hoặc các biện pháp tiếp nhận khác phải chỉ ra được thời gian gửi và phải kiểm tra được tính toàn vẹn của văn bản điện tử.
134. Văn bản điện tử của cơ quan nhà nước phải được đưa vào hồ sơ lưu trữ theo cách bảo đảm tính xác thực, an toàn và khả năng truy nhập văn bản điện tử đó.
135. Tất cả các phương án trên.
136. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Sử dụng chữ ký điện tử, nội dung nào sau đây là đúng?
137. Cơ quan nhà nước có trách nhiệm sử dụng chữ ký điện tử để xác nhận văn bản điện tử cuối cùng.
138. Chữ ký điện tử của cơ quan nhà nước phải đáp ứng các yêu cầu của pháp luật về giao dịch điện tử.
139. Tất cả các phương án trên.
140. Cả phương án a và b đều sai.
141. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Nguyên tắc bảo đảm an toàn thông tin, nội dung nào sau đây là đúng?
142. Thông tin số thuộc quy định danh mục bí mật nhà nước của các cơ quan nhà nước không phải được phân loại, lưu trữ, bảo vệ trên cơ sở quy định của pháp luật về bảo vệ bí mật nhà nước.
143. Thông tin số thuộc quy định danh mục bí mật nhà nước của các cơ quan nhà nước phải được phân loại, lưu trữ, bảo vệ trên cơ sở quy định của pháp luật về bảo vệ bí mật nhà nước.
144. Không cần sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã;
145. Không cần quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước;
146. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Điều kiện bảo đảm thực hiện nhiệm vụ an toàn thông tin, nội dung nào sau đây là đúng?
147. Cán bộ, công chức, viên chức phải nắm vững các quy định của pháp luật và nội quy của cơ quan về an toàn thông tin;
148. Cán bộ kỹ thuật về an toàn thông tin phải được tuyển chọn, đào tạo, huấn luyện, thường xuyên bồi dưỡng nghiệp vụ phù hợp với nhiệm vụ được giao và được tạo điều kiện làm việc phù hợp;
149. Cơ quan nhà nước ưu tiên sử dụng lực lượng kỹ thuật về an toàn thông tin của mình; khi cần thiết có thể sử dụng dịch vụ của các tổ chức bảo đảm an toàn thông tin đủ năng lực được Nhà nước công nhận;
150. Tất cả các phương án trên.
151. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Áp dụng quy trình quản lý an toàn hạ tầng kỹ thuật, nội dung nào sau đây là đúng?
152. Các giải pháp bảo vệ nhằm ngăn chặn và phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;
153. Áp dụng các công nghệ xác thực, cơ chế quản lý quyền truy cập và cơ chế ghi biên bản hoạt động của hệ thống để quản lý và kiểm tra việc truy cập mạng; Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ và máy trạm;
154. Theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại khỏi hệ thống; Các quy trình quản lý an toàn hạ tầng kỹ thuật khác.
155. Tất cả các phương án trên.
156. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Trách nhiệm người đứng đầu cơ quan nhà nước, nội dung nào sau đây là đúng?
157. Trực tiếp chỉ đạo và chịu trách nhiệm về hoạt động ứng dụng công nghệ thông tin trong lĩnh vực, địa phương và tổ chức, cơ quan của mình.
158. Chỉ đạo xây dựng kế hoạch 5 năm, phê duyệt kế hoạch hàng năm về ứng dụng công nghệ thông tin trong lĩnh vực, địa phương và tổ chức, cơ quan của mình.
159. Quyết định các biện pháp nhằm tổ chức thực hiện có hiệu quả kế hoạch ứng dụng công nghệ thông tin. Quyết định về tổ chức bộ máy, cán bộ và hoạt động của đơn vị chuyên trách công nghệ thông tin trong hệ thống tổ chức, cơ quan của mình.
160. Tất cả các phương án trên.
161. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Hệ thống chuyên trách về công nghệ thông tin trong cơ quan nhà nước, nội dung nào sau đây là đúng?
162. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ có trách nhiệm chỉ định một đơn vị trực thuộc làm nhiệm vụ chuyên trách về công nghệ thông tin trong ngành mình.
163. Cơ quan quản lý nhà nước về công nghệ thông tin ở các tỉnh, thành phố trực thuộc Trung ương là đơn vị chuyên trách về công nghệ thông tin trong địa phương mình.
164. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh quy định cụ thể chức năng, nhiệm vụ, tổ chức bộ máy và hoạt động của các đơn vị chuyên trách công nghệ thông tin thuộc ngành hoặc địa phương mình căn cứ theo quy định tại Điều 46 của Nghị định.
165. Tất cả các phương án trên.
166. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Chức năng, nhiệm vụ chính của đơn vị chuyên trách về công nghệ thông tin, nội dung nào sau đây là đúng?
167. Thu thập, lưu trữ, xử lý thông tin phục vụ sự chỉ đạo, điều hành của lãnh đạo.
168. Quản lý, vận hành, hướng dẫn sử dụng cơ sở hạ tầng thông tin phục vụ hoạt động chỉ đạo, điều hành, tác nghiệp của ngành hoặc địa phương; bảo đảm kỹ thuật, an toàn thông tin.
169. Xây dựng và duy trì hoạt động trang thông tin điện tử của ngành hoặc địa phương; tổ chức triển khai bảo đảm kỹ thuật cho việc cung cấp dịch vụ hành chính công.
170. Tất cả các phương án trên.
171. Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan nhà nước, quy định Bảo vệ thông tin cá nhân do cơ quan nhà nước nắm giữ trên môi trường mạng, nội dung nào sau đây là đúng?
172. Cơ quan nhà nước thu thập, xử lý và sử dụng thông tin cá nhân trên môi trường mạng phải thực hiện theo quy định tại Điều 21 của Luật Công nghệ thông tin.
173. Các biện pháp bảo vệ thông tin cá nhân bao gồm: thông báo mục đích sử dụng thông tin cá nhân; giám sát quá trình xử lý thông tin cá nhân; ban hành thủ tục kiểm tra, đính chính hoặc huỷ bỏ thông tin cá nhân; các biện pháp kỹ thuật khác.
174. Cơ quan nhà nước nắm giữ thông tin thuộc bí mật cá nhân phải có trách nhiệm bảo vệ những thông tin đó và chỉ được phép cung cấp, chia sẻ cho bên thứ ba có thẩm quyền trong những trường hợp nhất định theo quy định của pháp luật.
175. Tất cả các phương án trên.
176. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nội dung quản lý nhà nước về công nghệ thông tin, nội dung nào sau đây là đúng?
177. Xây dựng, tổ chức thực hiện chiến lược, quy hoạch, kế hoạch, chính sách ứng dụng và phát triển công nghệ thông tin.
178. Xây dựng, ban hành, tuyên truyền, phổ biến, tổ chức thực hiện văn bản quy phạm pháp luật, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật trong lĩnh vực công nghệ thông tin.
179. Xây dựng cơ chế, chính sách và các quy định liên quan đến sản phẩm, dịch vụ công ích trong lĩnh vực công nghệ thông tin.
180. Tất cả các phương án trên.
181. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định các quyền của Tổ chức, cá nhân tham gia phát triển công nghệ thông tin, nội dung nào sau đây là đúng?
182. Nghiên cứu và phát triển sản phẩm công nghệ thông tin. Sản xuất sản phẩm công nghệ thông tin; số hóa, duy trì và làm tăng giá trị các nguồn tài nguyên thông tin.
183. Tổ chức, cá nhân khi hoạt động kinh doanh trên môi trường mạng phải thông báo công khai trên môi trường mạng những thông tin có liên quan.
184. Bảo đảm quyền và lợi ích hợp pháp của chủ sở hữu cơ sở dữ liệu và không gây cản trở cho việc sử dụng cơ sở dữ liệu đó khi thực hiện hành vi tái sản xuất, phân phối, quảng bá, truyền đưa, cung cấp nội dung hợp thành cơ sở dữ liệu đó.
185. Trả lời theo thẩm quyền văn bản của tổ chức, cá nhân gửi đến cơ quan nhà nước thông qua môi trường mạng.
186. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định trách nhiệm của cơ quan nhà nước khi hoạt động trên môi trường mạng, nội dung nào sau đây là đúng?
187. Thông báo cho tổ chức, cá nhân có liên quan địa chỉ liên hệ của cơ quan đó trên môi trường mạng. Trả lời theo thẩm quyền văn bản của tổ chức, cá nhân gửi đến cơ quan nhà nước thông qua môi trường mạng.
188. Cung cấp trên môi trường mạng thông tin phục vụ lợi ích công cộng, thủ tục hành chính. Sử dụng chữ ký điện tử theo quy định của pháp luật về giao dịch điện tử. Bảo đảm độ tin cậy và bí mật của nội dung thông tin trong việc gửi, nhận văn bản trên môi trường mạng.
189. Tất cả các phương án trên.
190. Cả phương án a và b đều sai.
191. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Các hành vi bị nghiêm cấm, nội dung nào sau đây là đúng?
192. Không cản trở hoạt động hợp pháp hoặc hỗ trợ hoạt động bất hợp pháp về ứng dụng và phát triển công nghệ thông tin; cản trở bất hợp pháp hoạt động của hệ thống máy chủ tên miền quốc gia; phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.
193. Cản trở hoạt động hợp pháp hoặc hỗ trợ hoạt động bất hợp pháp về ứng dụng và phát triển công nghệ thông tin; cản trở bất hợp pháp hoạt động của hệ thống máy chủ tên miền quốc gia; phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.
194. Không kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, kích động dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc.
195. Không xâm phạm quyền sở hữu trí tuệ trong hoạt động công nghệ thông tin; sản xuất, lưu hành sản phẩm công nghệ thông tin trái pháp luật; giả mạo trang thông tin điện tử của tổ chức, cá nhân khác; tạo đường dẫn trái phép đối với tên miền của tổ chức, cá nhân sử dụng hợp pháp tên miền đó.
196. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nguyên tắc chung về hoạt động ứng dụng công nghệ thông tin, nội dung nào sau đây là đúng?
197. Tổ chức, cá nhân có quyền tiến hành các hoạt động ứng dụng công nghệ thông tin theo quy định của Luật này và các quy định khác của pháp luật có liên quan.
198. Việc ứng dụng công nghệ thông tin vào các hoạt động thuộc lĩnh vực kinh tế - xã hội, đối ngoại, quốc phòng, an ninh; hoạt động phòng, chống lụt, bão, thiên tai, thảm họa khác, cứu hộ, cứu nạn và các hoạt động khác được Nhà nước khuyến khích.
199. Tổ chức, cá nhân tiến hành hoạt động viễn thông, hoạt động phát thanh, truyền hình trên môi trường mạng phải thực hiện các quy định của pháp luật về viễn thông, báo chí và các quy định của Luật này.
200. Tất cả các phương án trên.
201. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Ưu tiên ứng dụng công nghệ thông tin trong trường hợp khẩn cấp, nội dung nào sau đây là sai?
202. Phục vụ phòng, chống lụt, bão, hỏa hoạn, thiên tai, thảm họa khác.
203. Phục kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước.
204. Phục vụ cấp cứu và phòng, chống dịch bệnh. Phục vụ cứu nạn, cứu hộ.
205. Phục vụ quốc phòng, an ninh, bảo đảm trật tự, an toàn xã hội, phòng, chống tội phạm.
206. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Quản lý và sử dụng thông tin số, nội dung nào sau đây là đúng?
207. Tổ chức, cá nhân được trích dẫn nội dung thông tin số của tổ chức, cá nhân khác trong trường hợp chủ sở hữu thông tin số đã có cảnh báo hoặc pháp luật quy định việc trích dẫn thông tin là không được phép.
208. Tổ chức, cá nhân không được trích dẫn nội dung thông tin số của tổ chức, cá nhân khác trong trường hợp chủ sở hữu thông tin số đã có cảnh báo hoặc pháp luật quy định việc trích dẫn thông tin là không được phép.
209. Trường hợp không được phép trích dẫn thông tin số, tổ chức, cá nhân có trách nhiệm nêu rõ nguồn của thông tin đó.
210. Cơ quan nhà nước có thẩm quyền không phải chịu trách nhiệm thực hiện các biện pháp bảo đảm việc truy nhập và sử dụng thuận lợi thông tin số.
211. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Công cụ tìm kiếm thông tin số, nội dung nào sau đây là đúng?
212. Công cụ tìm kiếm thông tin số là chương trình máy tính tiếp nhận yêu cầu tìm kiếm thông tin số, thực hiện việc tìm kiếm thông tin số và gửi lại thông tin số tìm kiếm được.
213. Nhà nước có chính sách khuyến khích tổ chức, cá nhân phát triển, cung cấp công cụ tìm kiếm thông tin số.
214. Tổ chức, cá nhân có trách nhiệm ngừng cung cấp cho tổ chức, cá nhân khác công cụ tìm kiếm đến các nguồn thông tin số trong trường hợp tự mình phát hiện hoặc được cơ quan nhà nước có thẩm quyền thông báo cho biết thông tin đó là trái pháp luật.
215. Tất cả các phương án trên.
216. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Theo dõi, giám sát nội dung thông tin số, nội dung nào sau đây là đúng?
217. Cơ quan nhà nước có thẩm quyền chịu trách nhiệm theo dõi, giám sát thông tin số; điều tra các hành vi vi phạm pháp luật xảy ra trong quá trình truyền đưa hoặc lưu trữ thông tin số.
218. Tổ chức, cá nhân tham gia ứng dụng công nghệ thông tin không phải chịu trách nhiệm theo dõi, giám sát thông tin số của tổ chức, cá nhân khác, điều tra các hành vi vi phạm pháp luật xảy ra trong quá trình truyền đưa hoặc lưu trữ thông tin số của tổ chức, cá nhân khác, trừ trường hợp cơ quan nhà nước có thẩm quyền yêu cầu.
219. Tất cả các phương án trên.
220. Cả phương án a và b đều sai.
221. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Lưu trữ, cung cấp thông tin cá nhân trên môi trường mạng, nội dung nào sau đây là đúng?
222. Cá nhân có quyền yêu cầu tổ chức, cá nhân lưu trữ thông tin cá nhân của mình trên môi trường mạng thực hiện việc kiểm tra, đính chính hoặc hủy bỏ thông tin đó.
223. Tổ chức, cá nhân không được cung cấp thông tin cá nhân của người khác cho bên thứ ba, trừ trường hợp pháp luật có quy định khác hoặc có sự đồng ý của người đó.
224. Cá nhân có quyền yêu cầu bồi thường thiệt hại do hành vi vi phạm trong việc cung cấp thông tin cá nhân.
225. Tất cả các phương án trên.
226. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nguyên tắc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là đúng?
227. Việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải được ưu tiên, bảo đảm tính công khai, minh bạch nhằm nâng cao hiệu lực, hiệu quả hoạt động của cơ quan nhà nước; tạo điều kiện để nhân dân thực hiện tốt quyền và nghĩa vụ công dân.
228. Việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải thúc đẩy chương trình đổi mới hoạt động của cơ quan nhà nước và chương trình cải cách hành chính.
229. Việc cung cấp, trao đổi thông tin phải bảo đảm chính xác và phù hợp với mục đích sử dụng. Quy trình, thủ tục hoạt động phải công khai, minh bạch.
230. Tất cả các phương án trên.
231. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nguyên tắc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là đúng?
232. Sử dụng thống nhất tiêu chuẩn, bảo đảm tính tương thích về công nghệ trong toàn bộ hệ thống thông tin của các cơ quan nhà nước.
233. Bảo đảm an ninh, an toàn, tiết kiệm và có hiệu quả.
234. Người đứng đầu cơ quan nhà nước phải chịu trách nhiệm về việc ứng dụng công nghệ thông tin thuộc thẩm quyền quản lý của mình.
235. Tất cả các phương án trên.
236. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Điều kiện để triển khai ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là đúng?
237. Cơ quan nhà nước có trách nhiệm chuẩn bị các điều kiện để triển khai ứng dụng công nghệ thông tin trong hoạt động của cơ quan mình.
238. Chính phủ quy định cụ thể các điều kiện bảo đảm cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; xây dựng và tổ chức thực hiện chương trình quốc gia về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước
239. Tất cả các phương án trên.
240. Cả phương án a và b đều sai.
241. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nội dung ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là đúng?
242. Xây dựng và sử dụng cơ sở hạ tầng thông tin phục vụ cho hoạt động của cơ quan nhà nước và hoạt động trao đổi, cung cấp thông tin giữa cơ quan nhà nước với tổ chức, cá nhân.
243. Xây dựng, thu thập và duy trì cơ sở dữ liệu phục vụ cho hoạt động của cơ quan và phục vụ lợi ích công cộng.
244. Xây dựng các biểu mẫu phục vụ cho việc trao đổi, cung cấp thông tin và lấy ý kiến góp ý của tổ chức, cá nhân trên môi trường mạng.
245. Tất cả các phương án trên.
246. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nội dung ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là sai?
247. Xây dựng, thực hiện kế hoạch đào tạo, nâng cao nhận thức và trình độ ứng dụng công nghệ thông tin của cán bộ, công chức.
248. Thực hiện hoạt động trên môi trường mạng theo quy định
249. Xây dựng và sử dụng cơ sở hạ tầng thông tin phục vụ cho hoạt động của cơ quan nhà nước và hoạt động trao đổi, cung cấp thông tin giữa cơ quan nhà nước với tổ chức, cá nhân.
250. Xây dựng các biểu mẫu không phục vụ cho việc trao đổi, cung cấp thông tin và lấy ý kiến góp ý của tổ chức, cá nhân trên môi trường mạng.
251. Theo bạn, cách nói nào đúng nhất khi nói về mạng cục bộ - LAN?
252. Là một hệ thống mạng dùng để kết nối các [máy trạm](https://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh) trong một phạm vi nhỏ (nhà ở, cơ quan, trường học,…). Các máy tính trong LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.
253. Là một hệ thống mạng dùng để kết nối các [máy tính](https://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh) trong một phạm vi nhỏ (nhà ở, cơ quan, trường học,…). Các máy tính trong LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ [tập tin](https://vi.wikipedia.org/wiki/T%E1%BA%ADp_tin), máy in, máy quét và một số thiết bị khác.
254. Là một hệ thống mạng dùng để kết nối không dây các [máy](https://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh) tính trong một phạm vi nhỏ (nhà ở, cơ quan, trường học,…). Các máy tính trong LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.
255. Là một hệ thống mạng dùng để kết nối có dây các [máy t](https://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh)ính trong một phạm vi nhỏ (nhà ở, cơ quan, trường học,…). Các máy tính trong LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.
256. Theo bạn, đâu là khái niệm đúng nhất khi nói về Internet?
257. Là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu [nối chuyển gói](https://vi.wikipedia.org/wiki/Chuy%E1%BB%83n_m%E1%BA%A1ch_g%C3%B3i) dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP). Hệ thống này bao gồm tất cả các mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu và các trường đại học, của người dùng cá nhân và các chính phủ trên toàn cầu.
258. Là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu [nối chuyển gói](https://vi.wikipedia.org/wiki/Chuy%E1%BB%83n_m%E1%BA%A1ch_g%C3%B3i) dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP).
259. Là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu [nối chuyển gói](https://vi.wikipedia.org/wiki/Chuy%E1%BB%83n_m%E1%BA%A1ch_g%C3%B3i) dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP). Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu và các trường đại học, của người dùng cá nhân và các chính phủ trên toàn cầu.
260. Là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu [nối chuyển gói](https://vi.wikipedia.org/wiki/Chuy%E1%BB%83n_m%E1%BA%A1ch_g%C3%B3i) dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IPv6). Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu và các trường đại học, của người dùng cá nhân và các chính phủ trên toàn cầu.
261. Mô hình OSI có mấy lớp?

|  |  |
| --- | --- |
| 1. 4 lớp 2. 5 lớp | 1. 6 lớp 2. 7 lớp |

1. Mô hình OSI là một mô hình kiến trúc cơ bản
2. Không dành riêng cho phần mềm hoặc phần cứng nào
3. Chỉ dành riêng cho phần cứng
4. Chỉ dành riêng cho phần mềm
5. Mô hình này có 4 lớp
6. Theo bạn, bộ định tuyến Router được thiết kế để chạy trên lớp nào thuộc mô hình OSI?

|  |  |
| --- | --- |
| 1. Lớp 1 2. Lớp 2 | 1. Lớp 3 2. Lớp 4 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của giao thức FTP?

|  |  |
| --- | --- |
| 1. 21 2. 22 | 1. 23 2. 80 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của giao thức https?

|  |  |
| --- | --- |
| 1. 80 2. 88 | 1. 443 2. 344 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của giao thức POP3?

|  |  |
| --- | --- |
| 1. 995 2. 994 | 1. 143 2. 110 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của giao thức SSH?

|  |  |
| --- | --- |
| 1. 21 2. 22 | 1. 23 2. 24 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của giao thức http?

|  |  |
| --- | --- |
| 1. 8080 2. 8008 | 1. 80 2. 08 |

1. Trong các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp C?

|  |  |
| --- | --- |
| 1. 10.119.10.119 2. 203.199.199.1 | 1. 224.203.10.0 2. 172.16.1.203 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp D?

|  |  |
| --- | --- |
| 1. 224.224.0.1 2. 242.224.0.0 | 1. 241.224.0.0 2. 223.224.0.1 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp B?

|  |  |
| --- | --- |
| 1. 192.168.1.1 2. 193.168.1.1 | 1. 126.172.0.1 2. 172.126.0.1 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp A?

|  |  |
| --- | --- |
| 1. 128.126.0.1 2. 126.192.0.1 | 1. 172.192.0.1 2. 172.126.0.1 |

1. Cho địa chỉ mạng con (subnet) sau: 203.162.1.0/24 bạn hãy cho biết, mạng này có thể định được bao nhiêu host?

|  |  |
| --- | --- |
| 1. 24 2. 64 | 1. 128 2. 254 |

1. Cho địa chỉ mạng con (subnet) sau: 172.18.1.0/28 bạn hãy cho biết, mạng này có thể định được bao nhiêu host?

|  |  |
| --- | --- |
| 1. 14 2. 15 | 1. 28 2. 27 |

1. Cho địa chỉ mạng con (subnet) sau: 10.118.168.0/30 bạn hãy cho biết, mạng này có thể định được bao nhiêu host?

|  |  |
| --- | --- |
| 1. 30 2. 3 | 1. 2 2. 1 |

1. Trong các địa chỉ IP dưới đây, theo bạn đâu là địa chỉ không dùng để định danh trên Internet?

|  |  |
| --- | --- |
| 1. 191.18.1.2 2. 172.18.1.2 | 1. 11.11.11.2 2. 222.254.245.2 |

1. Trong các địa chỉ IP dưới đây, theo bạn đâu là địa chỉ không dùng để định danh trên Internet?

|  |  |
| --- | --- |
| 1. 192.16.2.2 2. 193.16.2.2 | 1. 173.16.2.2 2. 174.16.2.2 |

1. Bạn muốn kiểm tra kết nối giữa hai máy tính trong cùng mạng cục bộ (LAN), lệnh nào sau đây đáp ứng yêu cầu của bạn?

|  |  |
| --- | --- |
| 1. IPCONFIG 2. TELNET | 1. PING 2. TRACERT |

1. Bạn muốn kết nối đến máy chủ trong LAN của cơ quan để thực hiện một số tác vụ quản trị máy chủ từ xa, bạn sẽ sử dụng lệnh nào sau đây?

|  |  |
| --- | --- |
| 1. TELNET 2. TRACERT | 1. IPCONFIG 2. CONNECT |

1. Để cấp địa chỉ IP cho các máy tính trong LAN, người ta sử dụng dịch vụ có giao thức nào?

|  |  |
| --- | --- |
| 1. DNS 2. DHCP | 1. IPSEC 2. HTTP |

1. Lệnh nào sau đây cho biết địa chỉ IP của máy tính trong Windows?

|  |  |
| --- | --- |
| 1. IP 2. TCP\_IP | 1. IPCONFIG 2. FTP |

1. Trong các phần mềm dưới đây, theo bạn đâu là phần mềm ảo hóa có thể cài đặt được trên máy tính cá nhân (PC)?

|  |  |
| --- | --- |
| 1. VMWare Workstation 2. Microsoft Hyper-V | 1. Visual Basic 2. Cả A và B |

1. Theo bạn, máy chủ thường dùng vào việc:
2. Cài đặt các phần mềm dùng chung trong một cơ quan, tổ chức
3. Cài đặt các dịch vụ mạng như (DNS, DHCP,…)
4. Quản lý tệp tin (file server)
5. Tất cả các đáp án trên.
6. Để triển khai một website trong mạng cục bộ của một cơ quan với tên miền HOME.EGOV.VN, theo bạn cần sử dụng máy chủ nào?

|  |  |
| --- | --- |
| 1. DNS Server 2. DHCP Server | 1. Firewall Server 2. IIS Server |

1. Cơ quan bạn có một máy chủ đã được cài sẵn hệ điều hành Windows Server 2012, để cài đặt một website viết bằng ASP.NET, theo bạn cần phải sử dụng phần mềm nào để cài đặt website này lên máy chủ?

|  |  |
| --- | --- |
| 1. DNS 2. IIS | 1. Apache 2. ASP.NET |

1. Theo bạn, thiết bị nào sau đây giúp định tuyến gói tin giữa các lớp mạng khác nhau trong hệ thống LAN của một cơ quan, tổ chức?

|  |  |
| --- | --- |
| 1. Swictch layer 3 2. Switch layer 2 | 1. Router 2. Cả A và C đều được |

1. Cho một đoạn cáp UTP CAT 5, theo bạn tại mỗi đầu sử dụng bao nhiêu cặp sợi để truyền, nhận tín hiệu?

|  |  |
| --- | --- |
| 1. 2 cặp truyền, 2 cặp nhận 2. 1 cặp truyền, một cặp nhận | 1. Cả A và B đều đúng 2. 1 cặp truyền, 2 cặp nhận |

1. Các kết nối phổ biến nhất được sử dụng với cáp UTP là:

|  |  |
| --- | --- |
| 1. RJ-11 2. RJ-45 | 1. RJ-48 2. RJ-54 |

1. Để bấm cáp UTP đạt chuẩn 100Mbps, ta chú ý xếp các sợi ruột theo quy tắc nào?

|  |  |
| --- | --- |
| 1. 1-2-3-4 2. 1-2-3-5 | 1. 1-2-3-6 2. 1-3-5-7 |

1. Mạng VLAN là:
2. Mạng LAN ảo, xác định theo sơ đồ logic, không theo vị trí mạng vật lý
3. Mạng dùng riêng ảo xác định trên mạng công cộng (public network)
4. Mạng cục bộ trong một tòa nhà
5. Mạng diện rộng liên kết các mạng LAN trong khu vực rộng
6. Phương tiện vật lý nào cho khoảng cách xa nhất đối với mạng Ethernet?
7. Cáp đồng trục
8. Cáp xoắn đôi UTP
9. Cáp quang đơn mode (Single-Mode)
10. Cáp quang đa mode (Multi-Mode)
11. Tiêu chuẩn cho mạng Ethernet là tiêu chuẩn nào sau đây?

|  |  |
| --- | --- |
| 1. IEEE 802.3 2. IEEE 802.4 | 1. IEEE 802.5 2. IEEE 802.6 |

1. Tiêu chuẩn cho mạng không dây Wi-Fi là tiêu chuẩn nào sau đây?

|  |  |
| --- | --- |
| 1. IEEE 802.3 2. IEEE 802.4 | 1. IEEE 802.11 2. IEEE 802.12 |

1. Các địa chỉ MAC (Media Access Control) sử dụng bao nhiêu bit?

|  |  |
| --- | --- |
| 1. 16 2. 32 | 1. 48 2. 64 |

1. Địa chỉ IPv4 sử dụng bao nhiêu bit?

|  |  |
| --- | --- |
| 1. 16 2. 32 | 1. 48 2. 64 |

1. Địa chỉ IPv6 sử dụng bao nhiêu bit?

|  |  |
| --- | --- |
| 1. 64 2. 128 | 1. 129 2. 254 |

1. Theo bạn, Broadcast là gì?
2. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến một số điểm nhất định trong cùng một mạng
3. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến hầu hết các điểm khác trong cùng một mạng
4. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến tối đa 32 điểm khác trong cùng một mạng
5. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến tất cả các điểm khác trong cùng một mạng
6. Cho mạng con 192.168.0.0/24, theo bạn đâu là địa chỉ broadcast của mạng này?

|  |  |
| --- | --- |
| 1. 192.168.0.254 2. 192.168.0.255 | 1. 192.168.0.0 2. 192.168.0.1 |

1. Theo bạn, khi kết nối hai mạng LAN của chi nhánh cách trụ sở chính từ 100m đến 1km thì phương pháp kết nối nào sau đây an toàn và ổn định nhất?
2. Sử dụng VPN thông qua môi trường Internet
3. Sử dụng mạng không dây kết nối điểm – điểm
4. Sử dụng cáp quang
5. Sử dụng cáp đồng
6. Các mật khẩu nào sau đây là khó phá nhất đối với một hacker?

|  |  |
| --- | --- |
| 1. Password123456 2. MatKhau12 | 1. !$aLtNb19 2. LaN2s |

1. Loại tập tin nào sau đây dễ có khả năng chứa virus nhất?

|  |  |
| --- | --- |
| 1. database.dat 2. bigpic.jpeg | 1. note.txt.docx 2. picture.gif.exe |

1. Tại sao nói địa chỉ IPv6 bảo mật hơn địa chỉ IPv4?
2. Địa chỉ IPv6 sử dụng nhiều bit hơn gây khó khăn khi rà quét nên bảo mật tốt hơn
3. Địa chỉ IPv6 mới ra đời, chưa nhiều người biết đến, trong đó có cả giới tin tặc, do đó nó bảo mật hơn
4. Địa chỉ IPv6 được thiết kế để tích hợp sẵn tính năng bảo mật trong giao thức, địa chỉ IPv4 không tích hợp sẵn tính năng này
5. IPv4 không hỗ trợ nhiều thiết bị bảo mật
6. Đâu không phải là biện pháp bảo mật mạng không dây?

|  |  |
| --- | --- |
| 1. Mã hóa WEP 2. VPN | 1. Mã hóa WPA 2. Mã hóa WPA2 |

1. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như: web server, FTP server, email server?

|  |  |
| --- | --- |
| 1. DMZ 2. VLAN | 1. VPN 2. Intranet |

1. Dịch vụ mạng nào cho phép các địa chỉ mạng bên trong được "che dấu"( hidden) khỏi các mạng bên ngoài và cho phép một số host của mạng bên trong sử dụng các địa chỉ trùng với mạng bên ngoài?

|  |  |
| --- | --- |
| 1. NAT 2. VPN | 1. VLAN 2. IP spoofing |

1. Loại tấn công nào luôn sử dụng nhiều hơn một máy tính để tấn công nạn nhân?

|  |  |
| --- | --- |
| 1. DoS 2. DDoS | 1. Cửa hậu (Backdoor) 2. Tấn công UDP |

1. Bạn hãy chỉ ra thứ tự có hệ số bảo mật từ cao đến thấp khi cấu hình các lớp mạng cho một cơ quan, doanh nghiệp, tổ chức?

|  |  |
| --- | --- |
| 1. LAN, Internet, DMZ 2. LAN, DMZ, Internet | 1. DMZ, LAN, Internet 2. DMZ, Internet, LAN |

1. Theo bạn, đâu không phải là nhà cung cấp dịch vụ, giải pháp an toàn, bảo mật cho hệ thống mạng máy tính?

|  |  |
| --- | --- |
| 1. Fortinet 2. BKAV | 1. Avalon 2. Nokia |

1. Trong phát triển phần mềm, yếu tố nào quan trọng nhất?
   1. Con người.
   2. Quy trình.
   3. Sản phầm.
   4. Thời gian.
2. Kỹ sư phần mềm không cần
   1. Kiến thức về phân tích thiết kế hệ thống.
   2. Kiến thức về cơ sở dữ liệu.
   3. Lập trình thành thạo bằng một ngôn ngữ lập trình.
   4. Kinh nghiệm quản lý dự án phần mềm.
3. Tính khả thi của phần mềm dựa vào các yếu tố sau:
   1. Nghiệp vụ và tiếp thị.
   2. Phạm vi, ràng buộc và thị trường.
   3. Công nghệ, tiền bạc, thời gian và tài nguyên.
   4. Kỹ năng và năng lực của nhà phát triển.
4. Phần mềm dự báo thời tiết thu thập các số liệu về nhiệt độ, độ ẩm, … xử lý tính toán để cho ra các dự báo thời tiết là 1 ví dụ của loại phần mềm:
   1. Phần mềm hệ thống (System software)
   2. Phần mềm trí tuệ nhân tạo (Artificial Intelligence Software)
   3. Phần mềm thời gian thực (Real time software)
   4. Phần mềm nghiệp vụ (Business software)
5. Phần mềm quản lý sinh viên của 1 trường là:
   1. Phần mềm hệ thống (System software)
   2. Phần mềm trí tuệ nhân tạo (Artificial Intelligence Software)
   3. Phần mềm thời gian thực (Real time software)
   4. Phần mềm nghiệp vụ (Business software)
6. Mô hình phát triển phần mềm xoắn ốc
   1. Kết thúc với việc xuất xưởng sản phẩm phần mềm
   2. Nhiều hỗn độn hơn với mô hình gia tăng
   3. Bao gồm việc đánh giá những rủi ro phần mềm trong mỗi vòng lặp
   4. Tất cả điều trên
7. Mô hình phát triển dựa vào thành phần
   1. Chỉ phù hợp cho thiết kế phần cứng máy tính
   2. Không thể hỗ trợ phát triển những thành phần sử dụng lại
   3. Dựa vào những kỹ thuật hỗ trợ đối tượng
   4. Không định chi phí hiệu quả bằng những độ đo phần mềm có thể định lượng
8. Để xây dựng mô hình hệ thống, kỹ sư phải quan tâm tới một trong những nhân tố hạn chế sau :
   1. Những giả định và những ràng buộc
   2. Ngân sách và phí tổn
   3. Những đối tượng và những hoạt động
   4. Lịch biểu và các mốc sự kiện
9. Trong kỹ thuật tiến trình nghiệp vụ, ba kiến trúc khác nhau được kiểm tra
   1. Hạ tầng kỹ thuật, dữ liệu, ứng dụng
   2. Hạ tầng tài chánh, tổ chức và truyền thông
   3. Cấu trúc báo cáo, cơ sở dữ liệu, mạng
   4. Cấu trúc dữ liệu, yêu cầu, hệ thống
10. Thành phần nào của kỹ thuật tiến trình nghiệp vụ là trách nhiệm của kỹ sư phần mềm
    1. Phân tích phạm vi nghiệp vụ
    2. Thiết kế hệ thống nghiệp vụ
    3. Kế hoạch sản phẩm
    4. Kế hoạch chiến lược thông tin
11. Những thành phần kiến trúc trong kỹ thuật sản phẩm là
    1. Dữ liệu, phần cứng, phần mềm, con người
    2. Dữ liệu, tài liệu, phần cứng, phần mềm
    3. Dữ liệu, phần cứng, phần mềm, thủ tục
    4. Tài liệu, phần cứng, con người, thủ tục
12. Đặc tả hệ thống mô tả
    1. Chức năng và hành vi của hệ thống dựa vào máy tính
    2. Việc thi hành của mỗi thành phần hệ thống được chỉ
    3. Chi tiết giải thuật và cấu trúc hệ thống
    4. Thời gian đòi hỏi cho việc giả lập hệ thống
13. Cách tốt nhất để đưa tới việc xem xét việc đánh giá yêu cầu là
    1. Kiểm tra lỗi mô hình hệ thống
    2. Nhờ khách hàng kiểm tra yêu cầu
    3. Gởi họ tới đội thiết kế và xem họ có sự quan tâm nào không
    4. Dùng danh sách các câu hỏi kiểm tra để kiểm tra mỗi yêu cầu
14. Sử dụng bảng lần vết giúp
    1. Debug chương trình dựa theo việc phát hiện lỗi thời gian thực
    2. Xác định việc biểu diễn những sự thi hành giải thuật
    3. Xác định, điều khiển và theo vết những thay đổi yêu cầu
    4. Không có mục nào
15. Mẫu mô hình hệ thống chứa thành phần
    1. Input
    2. Output
    3. Giao diện người dùng
    4. Tất cả mục trên
16. Tác vụ nào không được biểu diễn như là một phần của phân tích yêu cầu phần mềm
    1. Định giá và tổng hợp
    2. Mô hình hóa và thừa nhận vấn đề
    3. Lập kế hoạch và lịch biểu
    4. Đặc tả và xem xét
17. Đích của kỹ thuật đặc tả ứng dụng thuận tiện (FAST - facilitated application specification techniques) là nhờ người phát triển và khách hàng
    1. Xây dựng một nguyên mẫu nhanh chóng
    2. Học công việc lẫn nhau
    3. Làm việc với nhau để phát triển một tập những yêu cầu ban đầu
    4. Làm việc với nhau để phát triển những đặc tả phần mềm kỹ thuật
18. Ai là người không thích hợp để tham dự vào nhóm FAST (facilitated application specification techniques)
    1. Kỹ sư phần cứng và phần mềm
    2. Đại diện nhà sản xuất
    3. Đại diện thị trường
    4. Nhân viên tài chánh cao cấp
19. Những yêu cầu nào được quan tâm suốt QFD (quality function deployment)
    1. exciting requirements
    2. expected requirement
    3. normal requirements
    4. technology requirements
20. Phân tích giá trị được dẫn ra như là một phần của QFD (quality function deployment) nhằm xác định
    1. Chi phí của hoạt động đảm bảo chất lượng của dự án
    2. Chi phí quan hệ của những yêu cầu qua việc triển khai chức năng, tác vụ và thông tin
    3. Độ ưu tiên quan hệ của những yêu cầu qua việc triển khai chức năng, tác vụ và thông tin
    4. Kích thước của bản ý kiến khách hàng
21. Use-cases là một kịch bản mà mô tả
    1. Phần mềm thực hiện như thế nào khi được dùng trong một tình huống cho trước
    2. Những công cụ CASE sẽ được dùng như thế nào để xây dựng hệ thống
    3. Kế hoạch xây dựng cho sản phẩm phần mềm
    4. Những test-case cho sản phẩm phần mềm
22. Nội dung thông tin biểu diễn những đối tượng điều khiển và dữ liệu riêng biệt mà bao gồm những thông tin mà
    1. Cần thiết để trình bày tất cả output
    2. Được đòi hỏi cho việc xử lý lỗi
    3. Được đòi hỏi cho hoạt động tạo giao diện hệ thống
    4. Được biến đổi bởi phần mềm
23. Dòng thông tin biểu diễn cách thức mà dữ liệu và điều khiển
    1. Quan hệ với một dữ liệu và điều khiển khác
    2. Biến đổi khi mỗi lần dịch chuyển qua hệ thống
    3. Sẽ được thực thi trong thiết kế cuối cùng
    4. Không có mục nào
24. Cấu trúc thông tin biểu diển tổ chức nội của
    1. Những cấu trúc dữ liệu dùng để biểu diễn loại dữ liệu
    2. Mô hình bố trí nhân viên dự án
    3. Mô hình truyền thông dự án
    4. Những dữ liệu khác nhau và những mục điều khiển
25. Loại mô hình nào được tạo ra trong phân tích yêu cầu phần mềm
    1. Chức năng và hành vi
    2. Giải thuật và cấu trúc dữ liệu
    3. Kiến trúc và cấu trúc
    4. Tính tin cậy và tính sử dụng
26. Trong ngữ cảnh của phân tích yêu cầu, hai loại phân tách vấn đề là
    1. bottom-up và top-down
    2. horizontal and vertical
    3. subordinate và superordinate
    4. Không có mục nào
27. Khung nhìn (view) nào được quan tâm đầu tiên trong phân tich yêu cầu phần mềm
    1. actor view
    2. data view
    3. essential view
    4. implementation view
28. Tạo nguyên mẫu tiến hóa thường thích được dùng hơn tạo nguyên mẫu bỏ đi bởi vì
    1. Cho phép tái sử dụng nguyên mẫu đầu
    2. Không đòi hỏi làm việc nhiều với khách hàng
    3. Dễ dành thực hiện nhanh
    4. Nhiều tin cậy hơn
29. Những mục nào không là nguyên tắc cho việc biểu diễn yêu cầu
    1. Biểu đồ phải thu hẹp về số và toàn vẹn trong sử dụng
    2. Hình thức và nội dung biểu diễn thích hợp với nội dung
    3. Những biểu diễn phải có thể xem xét lại
    4. Dùng không hơn 7 màu dương và 2 màu âm trong biểu đồ
30. Mục nào không là một mục đích cho việc xây dựng một mô hình phân tích
    1. Xác định một tập những yêu cầu phần mềm
    2. Mô tả yêu cầu khách hàng
    3. Phát triển một giải pháp tóm tắt cho vấn đề
    4. Thiết lập một nền tảng cho thiết kế phần mềm
31. Sơ đồ luồng dữ liệu
    1. Đưa ra hình ảnh quan hệ giữa các đối tượng dữ liệu
    2. Đưa ra hình ảnh những chức năng biến đổi luồng dữ liệu
    3. Chỉ ra những quyết định logic chính khi chúng xuất hiện
    4. Chỉ ra sự tương tác của hệ thống với sự kiện bên ngoài
32. Biểu đồ quan hệ thực thể
    1. Đưa ra hình ảnh quan hệ giữa các đối tượng dữ liệu
    2. Đưa ra hình ảnh những chức năng biến đổi luồng dữ liệu
    3. Chỉ ra những quyết định logic chính khi chúng xuất hiện
    4. Chỉ ra sự tương tác của hệ thống với sự kiện bên ngoài
33. Biểu đồ dịch chuyển trạng thái
    1. Đưa ra hình ảnh về các đối tượng dữ liệu
    2. Đưa ra hình ảnh chức năng biến đổi luồng dữ liệu
    3. Chỉ ra hình ảnh dữ liệu được biến đổi như thế nào bởi hệ thống
    4. Chỉ ra những tương tác của hệ thống đối với sự kiện bên ngoài
34. Phân tích văn phạm của bản tường thuật xử lý là bước đầu tiên tốt nhất để tạo ra
    1. Tự điển dữ liệu
    2. Biểu đồ dòng dữ liệu
    3. Biểu đồ quan hệ thực thể
    4. Biểu đồ dịch chuyển trạng thái
35. Biểu đồ dòng điều khiển
    1. Cần thiết để mô hình những hệ thống hướng sự kiện
    2. Được đòi hỏi cho tất cả hệ thống
    3. Được dùng trong biểu đồ dòng dữ liệu
    4. Hữu dụng trong mô hình hóa giao diện người dùng
36. Từ điển dữ liệu chứa những mô tả của mỗi
    1. Mục cấu hình phần mềm
    2. Đối tượng dữ liệu phần mềm
    3. Biểu đồ phần mềm
    4. Hệ thống ký hiệu phần mềm
37. Mô hình thiết kế không quan tâm tới
    1. Kiến trúc
    2. Dữ liệu
    3. Giao diện
    4. Phạm vi dự án
38. Sự quan trọng của thiết kế phần mềm có thể được tóm tắt bằng từ đơn
    1. Accuracy
    2. Complexity
    3. Efficiency
    4. Quality
39. Một đặc trưng của thiết kế tốt là
    1. Cho thấy sự liên kết mạnh giữa các module
    2. Thực hiện tất cả yêu cầu trong phân tích
    3. Bao gồm những test case cho tất cả thành phần
    4. Kết hợp mã nguồn nhằm mục đích mô tả
40. Mục nào không là đặc trưng chung trong các phương pháp thiết kế
    1. Quản lý cấu hình
    2. Ký hiệu thành phần chức năng
    3. Nguyên tắc đánh giá chất lượng
    4. Heuristic tinh chế
41. Loại trừu tượng nào được dùng trong thiết kế phần mềm
    1. Điều khiển
    2. Dữ liệu
    3. Thủ tục
    4. Tất cả mục trên
42. Loại mô hình nào không được có trong kiến trúc phần mềm
    1. Dữ liệu
    2. Động
    3. Xử lý
    4. Cấu trúc
43. Cấp bậc điều khiển thể hiện
    1. Thứ tự quyết định
    2. Việc tổ chức của các module
    3. Sự lặp lại của những hoạt động
    4. Sự tuần tự của các tiến trình
44. Thủ tục phần mềm tập trung vào
    1. Cấp bậc điều khiển trong một cảm nhận trừu tượng hơn
    2. Xử lý chi tiết của mỗi module riêng biệt
    3. Xử lý chi tiết của mỗi tập module
    4. Quan hệ giữa điều khiển và thủ tục
45. Nguyên nhân của việc sinh lỗi do thiết kế mức thành phần trước khi thiết kế dữ liệu là
    1. Thiết kế thành phần thì phụ thuộc vào ngôn ngữ còn thiết kế dữ liệu thì không
    2. Thiết kế dữ liệu thì dễ thực hiện hơn
    3. Thiết kế dữ liệu thì khó thực hiện
    4. Cấu trúc dữ liệu thường ảnh hưởng tới cách thức mà thíết kế thành phần phải theo
46. Mục đích của tham chiếu chéo những yêu cầu (ma trận) trong tài liệu thiết kế là nhằm
    1. Cho phép người quản lý theo dõi năng suất của nhóm thiết kế
    2. Xác minh là tất cả các yêu cầu đã được xem xét trong thiết kế
    3. Chỉ ra chi phí kết hợp với mỗi yêu cầu
    4. Cung cấp cho việc thực thi tên của những nhà thiết kế cho mỗi yêu cầu
47. Mục nào không là một phần của kiến trúc phần mềm
    1. Chi tiết giải thuật
    2. Cơ sở dữ liệu
    3. Thiết kế dữ liệu
    4. Cấu trúc chương trình
48. Đặc trưng nào là đúng cho kho dữ liệu, không phải là cơ sở dữ liệu đặc trưng
    1. Hướng mức nghiệp vụ và kích thước lớn
    2. Thông tin đúng và hợp thời
    3. Tích hợp và không thường thay đổi
    4. Tất cả những mục trên
49. Mẫu kiến trúc nhấn mạnh tới những thành phần
    1. Ràng buộc
    2. Tập hợp những thành phần
    3. Mô hình ngữ nghĩa
    4. Tất cả những mục
50. Nhằm xác định những mẫu kiến trúc hay kết hợp những mẫu phù hợp nhất cho hệ thống đề nghị, kỹ thuật yêu cầu dùng để khám phá
    1. Giải thuật phức tạp
    2. Đặc trưng và ràng buộc
    3. Điều khiển và dữ liệu
    4. Những mẫu thiết kế
51. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nội dung ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là sai?
52. Không thiết lập trang thông tin điện tử phù hợp với quy định tại Điều 23 và Điều 28 của Luật này.
53. Không cung cấp, chia sẻ thông tin với cơ quan khác của Nhà nước.
54. Thực hiện việc cung cấp dịch vụ công trên môi trường mạng.
55. Tất cả các phương án trên.
56. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nội dung ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nội dung nào sau đây là sai?
57. Xây dựng, thực hiện kế hoạch đào tạo, nâng cao nhận thức và trình độ ứng dụng công nghệ thông tin của cán bộ, công chức.
58. Thực hiện hoạt động trên môi trường mạng theo quy định
59. Xây dựng và sử dụng cơ sở hạ tầng thông tin phục vụ cho hoạt động của cơ quan nhà nước và hoạt động trao đổi, cung cấp thông tin giữa cơ quan nhà nước với tổ chức, cá nhân.
60. Xây dựng các biểu mẫu không phục vụ cho việc trao đổi, cung cấp thông tin và lấy ý kiến góp ý của tổ chức, cá nhân trên môi trường mạng.
61. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Hoạt động của cơ quan nhà nước trên môi trường mạng, nội dung nào sau đây là đúng?
62. Cung cấp, trao đổi, thu thập thông tin với tổ chức, cá nhân;
63. Chia sẻ thông tin trong nội bộ và với cơ quan khác của Nhà nước;
64. Cung cấp các dịch vụ công và Các hoạt động khác theo quy định của Chính phủ.
65. Tất cả các phương án trên.
66. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Trang thông tin điện tử của cơ quan nhà nước phải đáp ứng các yêu cầu sau đây?
67. Bảo đảm cho tổ chức, cá nhân truy nhập thuận tiện. Hỗ trợ tổ chức, cá nhân truy nhập và sử dụng các biểu mẫu trên trang thông tin điện tử (nếu có).
68. Bảo đảm tính chính xác và sự thống nhất về nội dung của thông tin trên trang thông tin điện tử. Cập nhật thường xuyên và kịp thời thông tin trên trang thông tin điện tử.
69. Thực hiện quy định của pháp luật về bảo vệ bí mật nhà nước.
70. Tất cả các phương án trên.
71. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Trang thông tin điện tử của cơ quan nhà nước phải có những thông tin chủ yếu sau đây?
72. Quy trình, thủ tục hành chính được thực hiện bởi các đơn vị trực thuộc, tên của người chịu trách nhiệm trong từng khâu thực hiện quy trình, thủ tục hành chính, thời hạn giải quyết các thủ tục hành chính.
73. Thông tin tuyên truyền, phổ biến, hướng dẫn thực hiện pháp luật, chế độ, chính sách, chiến lược, quy hoạch chuyên ngành. Danh mục địa chỉ thư điện tử chính thức của từng đơn vị trực thuộc và cán bộ, công chức có thẩm quyền.
74. Tất cả các phương án trên.
75. Cả phương án a và b đều sai.
76. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nguyên tắc ứng dụng công nghệ thông tin trong thương mại, nội dung nào sau đây là đúng?
77. Tổ chức, cá nhân không có quyền ứng dụng công nghệ thông tin trong thương mại.
78. Hoạt động thương mại trên môi trường mạng không phải tuân thủ quy định của Luật này, pháp luật về thương mại và pháp luật về giao dịch điện tử.
79. Tất cả các phương án trên.
80. Cả phương án a và b đều sai.
81. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nguyên tắc ứng dụng công nghệ thông tin trong thương mại, nội dung nào sau đây là đúng?
82. Tổ chức, cá nhân có quyền ứng dụng công nghệ thông tin trong thương mại.
83. Hoạt động thương mại trên môi trường mạng phải tuân thủ quy định của Luật này, pháp luật về thương mại và pháp luật về giao dịch điện tử.
84. Tất cả các phương án trên.
85. Cả phương án a và b đều sai.
86. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Trang thông tin điện tử bán hàng phải bảo đảm các yêu cầu chủ yếu nào?
87. Cung cấp đầy đủ, chính xác thông tin về hàng hóa, dịch vụ, điều kiện giao dịch, thủ tục giải quyết tranh chấp và bồi thường thiệt hại;
88. Cung cấp cho người tiêu dùng thông tin về phương thức thanh toán an toàn và tiện lợi trên môi trường mạng;
89. Công bố các trường hợp người tiêu dùng có quyền hủy bỏ, sửa đổi thỏa thuận trên môi trường mạng.
90. Tất cả các phương án trên.
91. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Trang thông tin điện tử bán hàng, nội dung nào sau đây là đúng?
92. Tổ chức, cá nhân sở hữu trang thông tin điện tử bán hàng không phải chịu trách nhiệm về nội dung thông tin cung cấp trên trang thông tin điện tử, thực hiện quy định của Luật này và các quy định khác của pháp luật có liên quan về giao kết hợp đồng, đặt hàng, thanh toán, quảng cáo, khuyến mại.
93. Tổ chức, cá nhân sở hữu trang thông tin điện tử bán hàng chịu trách nhiệm về nội dung thông tin cung cấp trên trang thông tin điện tử, thực hiện quy định của Luật này và các quy định khác của pháp luật có liên quan về giao kết hợp đồng, đặt hàng, thanh toán, quảng cáo, khuyến mại.
94. Tất cả các phương án trên.
95. Cả phương án a và b đều sai.
96. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Cung cấp thông tin cho việc giao kết hợp đồng trên môi trường mạng, nội dung nào sau đây là đúng?
97. Trình tự thực hiện để tiến tới giao kết hợp đồng trên môi trường mạng;
98. Biện pháp kỹ thuật xác định và sửa đổi thông tin nhập sai;
99. Việc lưu trữ hồ sơ hợp đồng và cho phép truy nhập hồ sơ đó.
100. Tất cả các phương án trên.
101. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Thanh toán trên môi trường mạng, nội dung nào sau đây là đúng?
102. Nhà nước khuyến khích tổ chức, cá nhân thực hiện thanh toán trên môi trường mạng theo quy định của pháp luật.
103. Điều kiện, quy trình, thủ tục thanh toán trên môi trường mạng do cơ quan nhà nước có thẩm quyền quy định.
104. Tất cả các phương án trên.
105. Cả phương án a và b đều sai.
106. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Ứng dụng công nghệ thông tin trong lĩnh vực y tế, nội dung nào sau đây là đúng?
107. Nhà nước có chính sách khuyến khích ứng dụng công nghệ thông tin trong lĩnh vực y tế.
108. Tổ chức, cá nhân tiến hành hoạt động y tế trên môi trường mạng phải tuân thủ quy định của Luật này, pháp luật về y, dược và các quy định khác của pháp luật có liên quan.
109. Bộ Y tế quy định cụ thể điều kiện hoạt động y tế trên môi trường mạng.
110. Tất cả các phương án trên.
111. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Khuyến khích nghiên cứu - phát triển công nghệ thông tin, nội dung nào sau đây là đúng?
112. Nhà nước không khuyến khích tổ chức, cá nhân nghiên cứu - phát triển công nghệ, sản phẩm công nghệ thông tin nhằm phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh, nâng cao đời sống vật chất, tinh thần của nhân dân.
113. Tổ chức, cá nhân nghiên cứu - phát triển công nghệ, sản phẩm công nghệ thông tin để đổi mới quản lý kinh tế - xã hội, đổi mới công nghệ không được hưởng ưu đãi về thuế, tín dụng và các ưu đãi khác theo quy định của pháp luật.
114. Tất cả các phương án trên.
115. Cả phương án a và b đều sai.
116. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Nghiên cứu - phát triển công nghệ, sản phẩm công nghệ thông tin, nội dung nào sau đây là đúng?
117. Nhà nước ưu tiên dành một khoản từ ngân sách nhà nước cho các chương trình, đề tài nghiên cứu - phát triển phần mềm; ưu tiên hoạt động nghiên cứu - phát triển công nghệ thông tin ở trường đại học, viện nghiên cứu; phát triển các mô hình gắn kết nghiên cứu, đào tạo với sản xuất về công nghệ thông tin.
118. Cả phương án a và d đều đúng.
119. Cả phương án a và d đều sai.
120. Cơ quan quản lý nhà nước về công nghệ thông tin chủ trì, phối hợp với cơ quan quản lý nhà nước về khoa học và công nghệ tổ chức tuyển chọn cơ sở nghiên cứu, đào tạo, doanh nghiệp thực hiện nhiệm vụ nghiên cứu - phát triển sản phẩm công nghệ thông tin trọng điểm.
121. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Chất lượng sản phẩm, dịch vụ công nghệ thông tin được quản lý thông qua các hình thức nào?
122. Chứng nhận phù hợp tiêu chuẩn, quy chuẩn kỹ thuật;
123. Công bố phù hợp tiêu chuẩn, quy chuẩn kỹ thuật;
124. Kiểm định chất lượng.
125. Tất cả các phương án trên.
126. Theo Luật An ninh mạng 24/2018/QH14 quy định Biện pháp bảo vệ an ninh mạng, nội dung nào sau đây là đúng?
127. Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật.
128. Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
129. Tất cả các phương án trên.
130. Cả phương án a và b đều sai.
131. Theo Luật An ninh mạng 24/2018/QH14 quy định Biện pháp bảo vệ an ninh mạng, nội dung nào sau đây là đúng?
132. Không ứng phó, khắc phục sự cố an ninh mạng;
133. Đấu tranh bảo vệ an ninh mạng;
134. Không sử dụng mật mã để bảo vệ thông tin mạng;
135. Tất cả các phương án trên.
136. Theo Luật An ninh mạng 24/2018/QH14 quy định Bảo vệ không gian mạng quốc gia, nội dung nào sau đây là đúng?
137. Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; không phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.
138. Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.
139. Nhà nước không không áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; không phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.
140. Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, không bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.
141. Theo Luật An ninh mạng 24/2018/QH14 quy định Các hành vi bị nghiêm cấm về an ninh mạng, nội dung nào sau đây là đúng?
142. Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;
143. Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;
144. Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;
145. Tất cả các phương án trên.
146. Theo Luật An ninh mạng 24/2018/QH14 quy định Các hành vi bị nghiêm cấm về an ninh mạng, nội dung nào sau đây là sai?
147. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.
148. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.
149. Không lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.
150. Tất cả các phương án trên.
151. Theo Luật An ninh mạng 24/2018/QH14 quy định Hệ thống thông tin quan trọng về an ninh quốc gia, phát biểu nào sau đây là đúng?
152. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ không xâm phạm nghiêm trọng an ninh mạng.
153. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.
154. Hệ thống thông tin quan trọng về an ninh quốc gia không phải là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.
155. Hệ thống thông tin quan trọng về an ninh quốc gia không phải là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ không xâm phạm nghiêm trọng an ninh mạng.
156. Theo Luật An ninh mạng 24/2018/QH14 quy định Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như nào là đúng?
157. Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; ít nhất là 72 giờ trong trường hợp có yêu cầu quản lý nhà nước về an ninh mạng hoặc hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng.
158. Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin.
159. Tất cả các phương án trên.
160. Cả phương án a và b đều sai.
161. Theo Luật An ninh mạng 24/2018/QH14 quy định Hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm những nội dung nào sau đây?
162. Phát hiện, xác định sự cố an ninh mạng.
163. Bảo vệ hiện trường, thu thập chứng cứ.
164. Phong tỏa, giới hạn phạm vi xảy ra sự cố an ninh mạng, hạn chế thiệt hại do sự cố an ninh mạng gây ra.
165. Tất cả các phương án trên.
166. Theo Luật An ninh mạng 24/2018/QH14 quy định Hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm những nội dung nào sau đây?
167. Không xác định mục tiêu, đối tượng, phạm vi cần ứng cứu.
168. Không xác minh, phân tích, đánh giá, phân loại sự cố an ninh mạng.
169. Không xác minh nguyên nhân và truy tìm nguồn gốc.
170. Triển khai phương án ứng phó, khắc phục sự cố an ninh mạng;
171. Theo Luật An ninh mạng 24/2018/QH14 quy định Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trong trường hợp nào sau đây?
172. Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội;
173. Khi có đề nghị của chủ quản hệ thống thông tin.
174. Tất cả các phương án trên.
175. Cả phương án a và b đều sai.
176. Theo Luật An ninh mạng 24/2018/QH14 quy định Đối tượng kiểm tra an ninh mạng bao gồm những nội dung nào sau đây?
177. Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin;
178. Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin;
179. Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật.
180. Tất cả các phương án trên.
181. Theo Luật An ninh mạng 24/2018/QH14 quy định Bảo đảm nguồn nhân lực bảo vệ an ninh mạng, nội dung nào sau đây là đúng?
182. Công dân Việt Nam có kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin là nguồn lực cơ bản, chủ yếu bảo vệ an ninh mạng.
183. Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng.
184. Khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc nguy cơ đe dọa an ninh mạng, cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng.
185. Tất cả các phương án trên.
186. Theo Luật An ninh mạng 24/2018/QH14 quy định Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng, nội dung nào sau đây là đúng?
187. Công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng.
188. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao.
189. Ưu tiên phát triển cơ sở đào tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà nước và khu vực tư nhân, trong nước và ngoài nước.
190. Tất cả các phương án trên.
191. Theo Luật An ninh mạng 24/2018/QH14 quy định Giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng, nội dung nào sau đây là đúng?
192. Nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường, chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh.
193. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng.
194. Tất cả các phương án trên.
195. Cả phương án a và b đều sai.
196. Theo Luật An ninh mạng 24/2018/QH14 quy định Phổ biến kiến thức về an ninh mạng, nội dung nào sau đây là đúng?
197. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng.
198. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức.
199. Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.
200. Tất cả các phương án trên.
201. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Vai trò của cổng thông tin điện tử của cơ quan nhà nước, nội dung nào sau đây là đúng?
202. Cổng thông tin điện tử của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ là cổng tích hợp thông tin của toàn ngành, lĩnh vực do cơ quan quản lý và được tích hợp thông tin dịch vụ công trực tuyến của tất cả các cơ quan, đơn vị trực thuộc.
203. Cổng thông tin điện tử của Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương là cổng tích hợp thông tin các lĩnh vực quản lý nhà nước trên phạm vi địa bàn của tỉnh và được tích hợp thông tin dịch vụ công trực tuyến của tất cả cơ quan chuyên môn trực thuộc và Ủy ban nhân dân cấp huyện của tỉnh.
204. Thông tin đăng tải trên cổng thông tin điện tử của cơ quan nhà nước là thông tin chính thống của cơ quan nhà nước trên môi trường mạng.
205. Tất cả các phương án trên.
206. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Nguyên tắc cung cấp thông tin, nội dung nào sau đây là đúng?
207. Thông tin cung cấp trên cổng thông tin điện tử của cơ quan nhà nước phải đúng với quan điểm, chủ trương, đường lối của Đảng, chính sách và pháp luật của Nhà nước; phục vụ kịp thời trong công tác quản lý của cơ quan và nhu cầu khai thác thông tin của các tổ chức, cá nhân.
208. Thông tin cung cấp trên cổng thông tin điện tử phải tuân thủ các quy định của pháp luật về bảo vệ bí mật nhà nước, báo chí, sở hữu trí tuệ và quản lý thông tin trên Internet.
209. Việc đăng tải, trích dẫn, sử dụng lại thông tin trên cổng thông tin điện tử của cơ quan phải ghi rõ thông tin về tác giả, nguồn của thông tin.
210. Tất cả các phương án trên.
211. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Thông tin, báo cáo thống kê, nội dung nào sau đây là đúng?
212. Cổng thông tin điện tử của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ phải cung cấp thông tin thống kê về ngành, lĩnh vực quản lý.
213. Cổng thông tin điện tử của Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương phải cung cấp thông tin thống kê từ kết quả các cuộc điều tra theo quy định của Luật Thống kê.
214. Thông tin thống kê phải bao gồm đầy đủ số liệu, báo cáo thống kê, phương pháp thống kê và bản phân tích số liệu thống kê, thời gian thực hiện thống kê.
215. Tất cả các phương án trên.
216. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Thông tin tiếng nước ngoài, nội dung nào sau đây là đúng?
217. Đối với cổng thông tin điện tử của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương: tối thiểu các thông tin quy định tại điểm a và k khoản 1 Điều 10 của Nghị định này và các thông tin dịch vụ công trực tuyến mà người nước ngoài có thể sử dụng phải được cung cấp bổ sung bằng tiếng Anh để tham khảo.
218. Khuyến khích cơ quan chủ quản đăng tải các mục thông tin khác bằng tiếng Anh và các ngôn ngữ khác.
219. Tất cả các phương án trên.
220. Cả phương án a và b đều sai.
221. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Cung cấp dữ liệu đặc tả, nội dung nào sau đây là đúng?
222. Cổng thông tin điện tử của cơ quan nhà nước phải cung cấp các dữ liệu đặc tả để hỗ trợ tìm kiếm, trao đổi và chia sẻ thông tin, bảo đảm khả năng liên kết, tích hợp với cổng thông tin điện tử của cơ quan nhà nước khác, đồng thời bảo đảm sự tương thích về công nghệ.
223. Bộ Thông tin và Truyền thông có trách nhiệm hướng dẫn chi tiết việc áp dụng các tiêu chuẩn về dữ liệu đặc tả cho các cơ quan nhà nước.
224. Cả phương án a và b đều sai.
225. Tất cả các phương án trên.
226. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Chức năng hỗ trợ tìm kiếm, liên kết và lưu trữ thông tin, nội dung nào sau đây là đúng?
227. Cổng thông tin điện tử phải có chức năng tra cứu, tìm kiếm thông tin cho phép tìm kiếm được đầy đủ và chính xác nội dung thông tin, tin, bài cần tìm hiện có.
228. Cung cấp đầy đủ, chính xác các đường liên kết đến cổng thông tin điện tử của các đơn vị trực thuộc và cơ quan nhà nước khác.
229. Cung cấp chức năng in ấn và lưu trữ cho mỗi tin, bài.
230. Tất cả các phương án trên.
231. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Thông tin về dịch vụ công trực tuyến, nội dung nào sau đây là đúng?
232. Cơ quan chủ quản có trách nhiệm đăng tải toàn bộ thông tin về dịch vụ công trực tuyến trên Cơ sở dữ liệu quốc gia về thủ tục hành chính. Thông tin về dịch vụ công trực tuyến phải được cập nhật, bổ sung, chỉnh sửa kịp thời ngay sau khi có sự thay đổi.
233. Cổng thông tin điện tử của cơ quan nhà nước phải có mục “Dịch vụ công trực tuyến” thông báo danh mục các dịch vụ hành chính công và các dịch vụ công trực tuyến đang thực hiện và nêu rõ mức độ của dịch vụ. Các dịch vụ được tổ chức, phân loại theo ngành, lĩnh vực để thuận tiện cho việc khai thác sử dụng.
234. Cổng thông tin điện tử của cơ quan nhà nước phải cung cấp chức năng hướng dẫn sử dụng, theo dõi tần suất sử dụng, quá trình xử lý và số lượng hồ sơ đã được xử lý đối với từng dịch vụ công trực tuyến từ mức độ 3 trở lên.
235. Tất cả các phương án trên.
236. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Thông tin về dịch vụ công trực tuyến, nội dung nào sau đây là đúng?
237. Cơ quan chủ quản có trách nhiệm đăng tải toàn bộ thông tin về dịch vụ công trực tuyến trên Cơ sở dữ liệu quốc gia về thủ tục hành chính. Thông tin về dịch vụ công trực tuyến phải được cập nhật, bổ sung, chỉnh sửa kịp thời ngay sau khi có sự thay đổi.
238. Cổng thông tin điện tử của cơ quan nhà nước không phải có mục “Dịch vụ công trực tuyến” thông báo danh mục các dịch vụ hành chính công và các dịch vụ công trực tuyến đang thực hiện và nêu rõ mức độ của dịch vụ. Các dịch vụ được tổ chức, phân loại theo ngành, lĩnh vực để thuận tiện cho việc khai thác sử dụng.
239. Cổng thông tin điện tử của cơ quan nhà nước không phải cung cấp chức năng hướng dẫn sử dụng, theo dõi tần suất sử dụng, quá trình xử lý và số lượng hồ sơ đã được xử lý đối với từng dịch vụ công trực tuyến từ mức độ 3 trở lên.
240. Tất cả các phương án trên.
241. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Tích hợp thông tin dịch vụ công trực tuyến, nội dung nào sau đây là đúng?
242. Cổng thông tin điện tử của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ không cần liên kết, tích hợp thông tin dịch vụ công trực tuyến với các cổng thông tin điện tử của các đơn vị trực thuộc.
243. Cổng thông tin điện tử của Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương không phải liên kết, tích hợp thông tin dịch vụ công trực tuyến với cổng thông tin điện tử của các cơ quan chuyên môn trực thuộc và Ủy ban nhân dân cấp huyện trực thuộc.
244. Văn phòng Chính phủ là cơ quan đầu mối trong việc tổ chức tích hợp thông tin dịch vụ công trực tuyến trên tất cả các lĩnh vực quản lý nhà nước của Chính phủ.
245. Cả phương án a, b đều đúng
246. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Tích hợp thông tin dịch vụ công trực tuyến, nội dung nào sau đây là đúng?
247. Cổng thông tin điện tử của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ phải được liên kết, tích hợp thông tin dịch vụ công trực tuyến với các cổng thông tin điện tử của các đơn vị trực thuộc.
248. Cổng thông tin điện tử của Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương phải được liên kết, tích hợp thông tin dịch vụ công trực tuyến với cổng thông tin điện tử của các cơ quan chuyên môn trực thuộc và Ủy ban nhân dân cấp huyện trực thuộc.
249. Văn phòng Chính phủ là cơ quan đầu mối trong việc tổ chức tích hợp thông tin dịch vụ công trực tuyến trên tất cả các lĩnh vực quản lý nhà nước của Chính phủ.
250. Cả 3 phương án trên.
251. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Ban Biên tập cổng thông tin điện tử, nội dung nào sau đây là đúng?
252. Ban Biên tập cổng thông tin điện tử là bộ phận giúp việc cho Thủ trưởng cơ quan chủ quản trong việc tiếp nhận, xử lý, biên tập, cập nhật thông tin và phối hợp xử lý dịch vụ công để đảm bảo hoạt động của cổng thông tin điện tử. Bộ phận chuyên trách về công nghệ thông tin của cơ quan chủ quản là cơ quan thường trực của Ban Biên tập.
253. Quy mô và tổ chức của Ban Biên tập cổng thông tin điện tử do Thủ trưởng cơ quan chủ quản quyết định căn cứ trên tình hình thực tế.
254. Ban Biên tập cổng thông tin điện tử gồm có Trưởng Ban, Phó Trưởng Ban và các thành viên. Lãnh đạo Ban Biên tập có thể làm việc theo chế độ kiêm nhiệm. Chế độ làm việc của các thành viên do Thủ trưởng cơ quan chủ quản quyết định.
255. Cả 3 phương án trên.
256. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Mức chi tạo lập thông tin và chi trả nhuận bút, nội dung nào sau đây là đúng?
257. Chế độ thù lao, nhuận bút cho việc cung cấp thông tin trên cổng thông tin điện tử được hưởng chế độ nhuận bút theo quy định hiện hành.
258. Mức chi cho việc tạo lập, chuyển đổi và số hóa thông tin cho cổng thông tin điện tử thực hiện theo hướng dẫn của Bộ Tài chính về mức chi tạo lập thông tin điện tử.
259. Căn cứ khả năng kinh phí của cơ quan, Thủ trưởng cơ quan chủ quản quyết định mức chi cụ thể cho việc tạo lập thông tin và chi trả nhuận bút phù hợp với các quy định hiện hành của Nhà nước.
260. Cả 3 phương án trên.
261. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Bảo trì, bảo dưỡng, duy trì hoạt động, nâng cấp, chỉnh sửa cổng thông tin điện tử, nội dung nào sau đây là đúng?
262. Cổng thông tin điện tử phải được thường xuyên kiểm tra, bảo dưỡng, chỉnh sửa, giám sát hoạt động để bảo đảm hoạt động liên tục 24 giờ trong tất cả các ngày.
263. Hàng năm, cổng thông tin điện tử phải được rà soát, đề xuất phương án nâng cấp, chỉnh sửa cho phù hợp với nhu cầu thực tế.
264. Tất cả các phương án trên.
265. Cả phương án a và b đều sai.
266. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Bảo đảm đường truyền, máy móc, trang thiết bị phục vụ việc thu thập, xử lý thông tin, nội dung nào sau đây là đúng?
267. Cơ quan chủ quản lựa chọn phương án đầu tư xây dựng hạ tầng hoặc thuê dịch vụ từ nhà cung cấp bên ngoài để bảo đảm cho hoạt động của cổng thông tin điện tử theo nguyên tắc tiết kiệm chi phí và bảo đảm hiệu quả.
268. Cơ quan chủ quản có trách nhiệm trang bị đầy đủ trang thiết bị cần thiết phục vụ cho việc thu thập, xử lý và cập nhật thông tin cho cổng thông tin điện tử, bảo đảm khai thác hiệu quả hạ tầng công nghệ hiện có.
269. Tất cả các phương án trên.
270. Cả phương án a và b đều sai.
271. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Bảo đảm an toàn thông tin và dữ liệu, Cơ quan chủ quản có trách nhiệm nào sau đây?
272. Thực hiện các biện pháp kỹ thuật để bảo đảm an toàn thông tin và dữ liệu trên cổng thông tin điện tử.
273. Xây dựng giải pháp hiệu quả chống lại các tấn công gây mất an toàn thông tin của cổng thông tin điện tử.
274. Xây dựng phương án dự phòng khắc phục sự cố bảo đảm hệ thống cổng thông tin điện tử hoạt động liên tục ở mức tối đa.
275. Tất cả các phương án trên.
276. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Bảo đảm đường truyền, máy móc, trang thiết bị phục vụ việc thu thập, xử lý thông tin, nội dung nào sau đây là đúng?
277. Cơ quan chủ quản lựa chọn phương án đầu tư xây dựng hạ tầng hoặc thuê dịch vụ từ nhà cung cấp bên ngoài để bảo đảm cho hoạt động của cổng thông tin điện tử theo nguyên tắc tiết kiệm chi phí và bảo đảm hiệu quả.
278. Cơ quan chủ quản không có trách nhiệm trang bị đầy đủ trang thiết bị cần thiết phục vụ cho việc thu thập, xử lý và cập nhật thông tin cho cổng thông tin điện tử, bảo đảm khai thác hiệu quả hạ tầng công nghệ hiện có.
279. Cả phương án a và b đều sai.
280. Tất cả các phương án trên.
281. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Bảo trì, bảo dưỡng, duy trì hoạt động, nâng cấp, chỉnh sửa cổng thông tin điện tử, nội dung nào sau đây là đúng?
282. Cổng thông tin điện tử không cần thường xuyên kiểm tra, bảo dưỡng, chỉnh sửa, giám sát hoạt động để bảo đảm hoạt động liên tục 24 giờ.
283. Hàng năm, cổng thông tin điện tử không cần rà soát, đề xuất phương án nâng cấp, chỉnh sửa cho phù hợp với nhu cầu thực tế.
284. Tất cả các phương án trên.
285. Cả phương án a và b đều sai.
286. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Tích hợp thông tin dịch vụ công trực tuyến, nội dung nào sau đây là đúng?
287. Cổng thông tin điện tử của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ không phải liên kết, tích hợp thông tin dịch vụ công trực tuyến với các cổng thông tin điện tử của các đơn vị trực thuộc.
288. Cổng thông tin điện tử của Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương phải được liên kết, tích hợp thông tin dịch vụ công trực tuyến với cổng thông tin điện tử của các cơ quan chuyên môn trực thuộc và Ủy ban nhân dân cấp huyện trực thuộc.
289. Văn phòng Chính phủ không phải là cơ quan đầu mối trong việc tổ chức tích hợp thông tin dịch vụ công trực tuyến trên tất cả các lĩnh vực quản lý nhà nước của Chính phủ.
290. Cả 3 phương án trên.
291. Theo nghị định số 43/2011/NĐ-CP ngày 13/6/2011 Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử, quy định về Nguyên tắc cung cấp thông tin, nội dung nào sau đây là đúng?
292. Thông tin cung cấp trên cổng thông tin điện tử của cơ quan nhà nước phải đúng với quan điểm, chủ trương, đường lối của Đảng, chính sách và pháp luật của Nhà nước; phục vụ kịp thời trong công tác quản lý của cơ quan và nhu cầu khai thác thông tin của các tổ chức, cá nhân.
293. Thông tin cung cấp trên cổng thông tin điện tử không phải tuân thủ các quy định của pháp luật về bảo vệ bí mật nhà nước, báo chí, sở hữu trí tuệ và quản lý thông tin trên Internet.
294. Việc đăng tải, trích dẫn, sử dụng lại thông tin trên cổng thông tin điện tử của cơ quan không phải ghi rõ thông tin về tác giả, nguồn của thông tin.
295. Tất cả các phương án trên.
296. Theo Luật Công nghệ thông tin ngày 29/6/2006 quy định Lưu trữ, cung cấp thông tin cá nhân trên môi trường mạng, nội dung nào sau đây là đúng?
297. Cá nhân không có quyền yêu cầu tổ chức, cá nhân lưu trữ thông tin cá nhân của mình trên môi trường mạng thực hiện việc kiểm tra, đính chính hoặc hủy bỏ thông tin đó.
298. Tổ chức, cá nhân không được cung cấp thông tin cá nhân của người khác cho bên thứ ba, trừ trường hợp pháp luật có quy định khác hoặc có sự đồng ý của người đó.
299. Cá nhân không có quyền yêu cầu bồi thường thiệt hại do hành vi vi phạm trong việc cung cấp thông tin cá nhân.
300. Tất cả các phương án trên.
301. Mô hình TCP/IP có mấy lớp?

|  |  |
| --- | --- |
| 1. 1 lớp 2. 2 lớp | 1. 4 lớp 2. 8 lớp |

1. Theo bạn, phát biểu nào sau đây đúng nhất khi nói về thiết bị chuyển mạch (Switch)?
2. Kết nối các máy tính trong mạng cục bộ (LAN)
3. Kết nối các máy tính trong mạng diện rộng cách xa nhau về mặt địa lý
4. Hoạt động từ lớp 1 đến lớp 7 trong mô hình OSI
5. Được thiết kế để hoạt động tại lớp 3 trong mô hình OSI
6. Theo bạn, đâu là cổng dịch vụ mặc định của dịch vụ SMTP?

|  |  |
| --- | --- |
| 1. 21 2. 22 | 1. 23 2. 25 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của dịch vụ DNS?

|  |  |
| --- | --- |
| 1. 22 2. 52 | 1. 53 2. 553 |

1. Theo bạn, đâu là cổng dịch vụ mặc định của dịch vụ FTP?

|  |  |
| --- | --- |
| 1. 21 2. 22 | 1. 23 2. 24 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp C?

|  |  |
| --- | --- |
| 1. 192.168.1.1 2. 172.168.1.1 | 1. 12.118.168.1 2. 232.168.1.1 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp D?

|  |  |
| --- | --- |
| 1. 192.168.0.1 2. 172.18.1.1 | 1. 232.168.1.1 2. 222.168.1.1 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp B?

|  |  |
| --- | --- |
| 1. 192.168.2.1 2. 230.168.2.1 | 1. 220.168.2.1 2. 172.168.2.1 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp A?

|  |  |
| --- | --- |
| 1. 10.118.168.1 2. 192.168.0.1 | 1. 172.168.0.1 2. 128.118.168.1 |

1. Cho địa chỉ mạng con (subnet): 192.168.2.0/24 bạn hãy cho biết, mạng này có thể định được tối đa bao nhiêu host?

|  |  |
| --- | --- |
| 1. 64 2. 128 | 1. 254 2. 255 |

1. Cho địa chỉ mạng con (subnet): 10.118.168.0/26 bạn hãy cho biết, mạng này có thể định được tối đa bao nhiêu host?

|  |  |
| --- | --- |
| 1. 30 2. 32 | 1. 62 2. 64 |

1. Cho địa chỉ mạng con (subnet): 172.18.1.0/28 bạn hãy cho biết, mạng này có thể định được tối đa bao nhiêu host?

|  |  |
| --- | --- |
| 1. 14 2. 16 | 1. 30 2. 32 |

1. Trong các địa chỉ IP dưới đây, theo bạn đâu là địa chỉ không dùng để định danh trên Internet?

|  |  |
| --- | --- |
| 1. 10.118.118.2 2. 117.118.118.2 | 1. 118.10.118.2 2. 194.168.1.2 |

1. Trong các địa chỉ IP dưới đây, theo bạn đâu là địa chỉ riêng (Private IP) chỉ dùng định danh trong mạng riêng của cơ quan, tổ chức, doanh nghiệp?

|  |  |
| --- | --- |
| 1. 117.117.117.1 2. 118.118.118.1 | 1. 119.119.119.1 2. 10.10.10.1 |

1. Bạn muốn kiểm tra kết nối giữa hai máy tính trong cùng mạng cục bộ (LAN), lệnh nào sau đây đáp ứng yêu cầu của bạn?

|  |  |
| --- | --- |
| 1. IPCONFIG 2. PING | 1. TELNET 2. HOST |

1. Bạn muốn kết nối đến máy chủ trong LAN của cơ quan để thực hiện một số tác vụ quản trị máy chủ từ xa, bạn sẽ sử dụng lệnh nào sau đây?

|  |  |
| --- | --- |
| 1. TRACERT 2. IPCONFIG | 1. TELNET 2. CONNECT |

1. Để cấp địa chỉ IP trong LAN, người ta sử dụng dịch vụ có giao thức nào?

|  |  |
| --- | --- |
| 1. DNS 2. DHCP | 1. SMTP 2. HTTP |

1. Lệnh nào sau đây cho biết địa chỉ IP của máy tính trong Windows?

|  |  |
| --- | --- |
| 1. IP 2. TCP\_IP | 1. IPCONFIG 2. HOST |

1. Trong các phần mềm dưới đây, theo bạn đâu là phần mềm ảo hóa có thể cài đặt được trên máy tính cá nhân (PC)?

|  |  |
| --- | --- |
| 1. VMWare Workstation 2. Visual Basic | 1. Microsoft Hyper-V 2. Cả A và C |

1. Theo bạn, máy chủ thường dùng vào việc:
2. Cài đặt các ứng dụng dùng chung trong một cơ quan, tổ chức
3. Cài đặt các dịch vụ mạng như (DNS, DHCP,…)
4. Quản lý tệp tin (file server)
5. Tất cả các đáp án trên.
6. Để triển khai một website trong mạng cục bộ của một cơ quan với tên miền WEB.EGOV.VN, theo bạn cần sử dụng máy chủ nào?

|  |  |
| --- | --- |
| 1. DHCP Server 2. Firewall Server | 1. DNS Server 2. File Server |

1. Cơ quan bạn có một máy chủ đã được cài sẵn hệ điều hành Windows Server 2012, để cài đặt một website viết bằng PHP, theo bạn cần phải sử dụng phần mềm nào để cài đặt website này lên máy chủ?

|  |  |
| --- | --- |
| 1. DNS 2. IIS hoặc Apache | 1. Visual Studio 2. NET Framework |

1. Theo bạn, thiết bị nào sau đây giúp định tuyến gói tin giữa các lớp mạng khác nhau trong hệ thống LAN của một cơ quan, tổ chức?

|  |  |
| --- | --- |
| 1. Switch layer 2 2. Swictch layer 3 | 1. Router 2. Cả B và C đều được |

1. Cho một đoạn cáp UTP CAT 5, theo bạn tại mỗi đầu sử dụng bao nhiêu cặp sợi để truyền, nhận tín hiệu?

|  |  |
| --- | --- |
| 1. 2 cặp truyền, 2 cặp nhận 2. 1 cặp truyền, một cặp nhận | 1. 1 cặp truyền, 2 cặp nhận 2. Cả A và B đều đúng |

1. Các kết nối phổ biến nhất được sử dụng với cáp UTP là:

|  |  |
| --- | --- |
| 1. RJ-11 2. RJ-45 | 1. RJ-48 2. RJ-54 |

1. Để bấm cáp UTP đạt chuẩn 100Mbps, ta chú ý xếp các sợi ruột theo quy tắc nào?

|  |  |
| --- | --- |
| 1. 1-2-3-4 2. 2-4-6-8 | 1. 1-2-3-6 2. 1-3-5-7 |

1. Chọn đáp án đúng nhất khi nói về mạng VLAN?
2. Là mạng dùng riêng ảo xác định trên mạng công cộng (public network)
3. Là mạng LAN ảo, xác định theo sơ đồ logic, không theo vị trí mạng vật lý
4. Là mạng cục bộ trong một tòa nhà
5. Là mạng diện rộng liên kết các mạng LAN trong khu vực rộng
6. Phương tiện vật lý nào cho khoảng cách xa nhất đối với mạng Ethernet?
7. Cáp quang đơn mode (Single-Mode)
8. Cáp quang đa mode (Multi-Mode)
9. Cáp đồng trục
10. Cáp xoắn đôi UTP
11. Tiêu chuẩn cho mạng Ethernet là tiêu chuẩn nào sau đây?

|  |  |
| --- | --- |
| 1. IEEE 802.6 2. IEEE 802.5 | 1. IEEE 802.4 2. IEEE 802.3 |

1. Tiêu chuẩn cho mạng không dây Wi-Fi là tiêu chuẩn nào sau đây?

|  |  |
| --- | --- |
| 1. IEEE 802.2 2. IEEE 802.3 | 1. IEEE 802.11 2. IEEE 802.16 |

1. Các địa chỉ MAC (Media Access Control) sử dụng bao nhiêu bit?

|  |  |
| --- | --- |
| 1. 32 2. 46 | 1. 47 2. 48 |

1. Địa chỉ IPv4 sử dụng bao nhiêu bit?

|  |  |
| --- | --- |
| 1. 16 2. 32 | 1. 128 2. 129 |

1. Địa chỉ IPv6 sử dụng bao nhiêu bit?

|  |  |
| --- | --- |
| 1. 128 2. 129 | 1. 30 2. 32 |

1. Theo bạn, Broadcast là gì?
2. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến một số điểm nhất định trong cùng một mạng
3. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến hầu hết các điểm khác trong cùng một mạng
4. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến tất cả các điểm khác trong cùng một mạng
5. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến tối đa 32 điểm khác trong cùng một mạng
6. Cho mạng con 10.10.10.0/24, theo bạn đâu là địa chỉ broadcast của mạng này?

|  |  |
| --- | --- |
| 1. 10.10.10.0 2. 10.10.10.1 | 1. 10.10.10.254 2. 10.10.10.255 |

1. Cho mạng con 10.118.169.0/24, theo bạn đâu là địa chỉ host thuộc mạng này?

|  |  |
| --- | --- |
| 1. 10.118.169.0 2. 10.118.169.1 | 1. 10.118.170.0 2. 10.118.170.1 |

1. Cho mạng con 10.118.168.0/26, theo bạn địa chỉ nào không là địa chỉ host thuộc mạng này?

|  |  |
| --- | --- |
| 1. 10.118.168.60 2. 10.118.168.62 | 1. 10.118.168.63 2. 10.118.168.61 |

1. Cho mạng con 172.16.0.0/22, theo bạn địa chỉ nào không là địa chỉ host thuộc mạng này?

|  |  |
| --- | --- |
| 1. 172.16.1.254 2. 172.16.2.254 | 1. 172.16.3.254 2. 172.16.4.254 |

1. Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm hệ điều hành?
2. Cài đặt bản service pack mới nhất
3. Cài đặt lại HĐH thông dụng
4. Sao lưu hệ thống thường xuyên
5. Shut down hệ thống khi không sử dụng
6. Một người dùng vừa mua phải một máy tính xách tay đã nhiễm virus, trên máy không chứa phần mềm Antivirus và chưa được kết nối với mạng. Theo bạn, cách tốt nhất để xử lý máy tính xách tay này là gì?
7. Nối mạng máy tính xách tay và download phần mềm antivirus từ máy chủ
8. Khởi động máy tính xách tay với đĩa khởi động Antivirus mới nhất
9. Nối mạng máy tính xách tay và download phần mềm Antivirus từ Internet
10. Kết nối máy tính xách tay đến một máy tính cá nhân khác và diệt virus từ đó
11. Giao thức nào sau đây là một giao thức mạng dùng để thiết lập kết nối mạng một cách bảo mật?

|  |  |
| --- | --- |
| 1. Telnet 2. SSH | 1. HTTP 2. IP |

1. Các phát biểu sau đây, phát biểu nào tốt nhất mô tả một hacker mũ trắng?

|  |  |
| --- | --- |
| 1. Chuyên gia bảo mật 2. Cựu Hacker mũ đen | 1. Cựu Hacker mũ xám 2. Hacker hiểm độc |

1. 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 (ví dụ như Internet)?

|  |  |
| --- | --- |
| 1. Điểm truy cập không dây 2. Router | 1. Tường lửa 2. Switch |

1. Ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng ?

|  |  |
| --- | --- |
| 1. IDS 2. FTP | 1. Router 2. Sniffer |

1. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như: web server, FTP server, email server?

|  |  |
| --- | --- |
| 1. DMZ 2. VLAN | 1. VPN 2. Intranet |

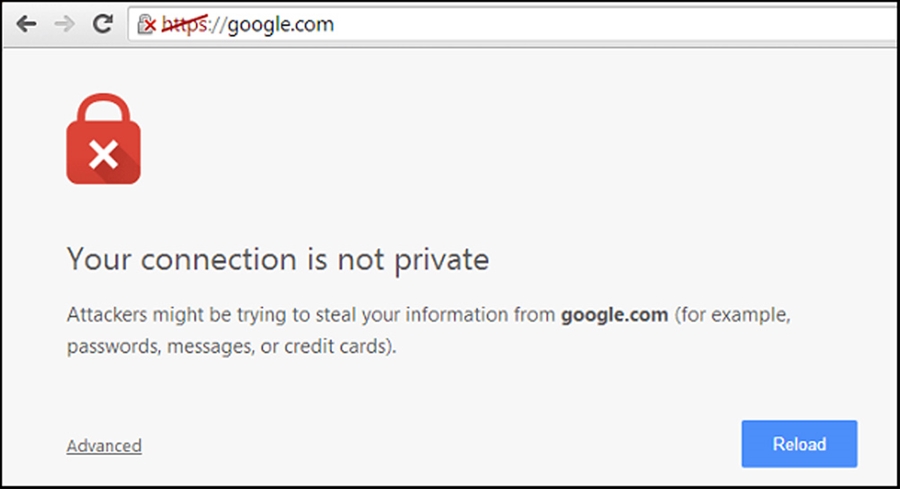
1. Dịch vụ mạng nào cho phép các địa chỉ mạng bên trong được "che dấu" (hidden) khỏi các mạng bên ngoài và cho phép một số host của mạng bên trong sử dụng các địa chỉ trùng với mạng bên ngoài?

|  |  |
| --- | --- |
| 1. VPN 2. VLAN | 1. IP spoofing 2. NAT |

1. 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?
2. Mã độc dạng Ransomware đã phát lệnh mã hóa các tập tin trên ổ cứng.
3. Một virus đang phát tán rộng trong hệ thống
4. Hệ thống của bạn đang chịu tác động của tấn công DoS
5. A, B đều có thể thuộc diện nghi ngờ
6. 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?
7. 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
8. Mở chương trình và chạy nó ngay. Chương trình đó thật sự an toàn vì nó được gửi từ Microsoft
9. Xoá email đó ngay. Microsoft và các nhà cung cấp không bao giờ gửi chương trình sửa lỗi qua email.
10. Tất cả đều sai
11. Khi cung cấp kết nối không dây (Wi-Fi) trong cơ quan, đơn vị bạn. Việc chia tách phần mạng Wi-Fi riêng ở một lớp mạng khác để tăng tính bảo mật mạng, tại thiết bị AccessPoint bạn nên làm như thế nào?
12. Nối cổng WAN vào nút mạng bất kỳ của cơ quan, đơn vị
13. Nối cổng LAN vào nút mạng bất kỳ của cơ quan, đơn vị
14. Thiết lập tường lửa trên AccessPoint
15. Đặt mật khẩu truy cập trên AccessPoint
16. Bạn hãy chỉ ra thứ tự có hệ số bảo mật từ cao đến thấp khi cấu hình các lớp mạng cho một cơ quan, doanh nghiệp, tổ chức?

|  |  |
| --- | --- |
| 1. LAN, WAN, Internet, DMZ 2. Internet, WAN, DMZ, LAN | 1. LAN, WAN, DMZ, Internet 2. DMZ, LAN, WAN, Internet |

1. Tiêu chuẩn đánh giá chất lượng của một thiết kế kiến trúc phải dựa vào
   1. Tính truy cập và tính tin cậy của hệ thống
   2. Dữ liệu và điều khiển của hệ thống
   3. Tính chức năng của hệ thống
   4. Những chi tiết thực thi của hệ thống
2. Trong phương pháp phân tích kiến trúc, mô tả mẫu kiến trúc thường dùng khung nhìn
   1. Dòng dữ liệu
   2. Module
   3. Tiến trình
   4. Tất cả các mục trên
3. Khi một luồng tổng thể trong một đoạn của biểu đồ luồng dữ liệu có tính trình tự cao và theo sau những những đường thẳng sẽ thể hiện
   1. Liên kết thấp
   2. Module hóa tốt
   3. Luồng giao dịch (transaction)
   4. Luồng biến đổi (transform)
4. Khi luồng thông tin trong một đoạn của sơ đồ luồng dữ liệu thể hiện bằng một mục đơn mà bẩy một luồng dữ liệu khác theo một trong nhiều đường sẽ thể hiện
   1. Liên kết thấp
   2. Module hóa tốt
   3. Luồng giao dịch (transaction)
   4. Luồng biến đổi (transform)
5. Một bổ sung cần thiết nhằm biến đổi hay ánh xạ giao dịch để tạo một thiết kế kiến trúc đầy đủ là
   1. Sơ đồ quan hệ - thực thể
   2. Từ điển dữ liệu
   3. Mô tả việc xử lý cho mỗi module
   4. Những Test-case cho mỗi module
6. Những nguyên lý thiết kế giao diện nào không cho phép người dùng còn điều khiển tương tác với máy tính
   1. Cho phép được gián đoạn
   2. Cho phép tương tác có thể undo
   3. Che dấu những bản chất kỹ thuật với những người dùng thường
   4. Chỉ cung cấp một cách thức xác định cứng khi hoàn thành tác vụ
7. Những nguyên lý thiết kế giao diện cho phép người dùng ít phải nhớ
   1. Xác định những shortcut trực quan
   2. Biểu lộ thông tin theo cách diễn tiến
   3. Thiết lập những trường hợp mặc định có ý nghĩa
   4. Tất cả những mục trên
8. Sự toàn vẹn (consistency) giao diện ngầm định
   1. Những kỹ thuật input giữ tương tự suốt ứng dụng
   2. Mỗi ứng dụng phải có look and feel riêng biệt
   3. Cách thức điều hướng (navigational) nhạy với ngữ cảnh
   4. Câu a và b
9. Mô hình nào đưa ra hình ảnh tiền sử (profile) người dùng cuối của hệ thống dựa vào máy tính
   1. Mô hình thiết kế
   2. Mô hình người dùng
   3. Mô hình của người dùng
   4. Mô hình nhận thức hệ thống
10. Mô hình nào đưa ra hình ảnh hệ thống trong đầu của người dùng cuối
    1. Mô hình thiết kế
    2. Mô hình người dùng
    3. Hình ảnh hệ thống
    4. Mô hình nhận thức hệ thống
11. Mô hình nào đưa ra hình ảnh look and feel cho giao diện người dùng cùng những thông tin hỗ trợ
    1. Mô hình thiết kế
    2. Mô hình người dùng
    3. Mô hình hình ảnh hệ thống
    4. Mô hình nhận thức hệ thống
12. Những hoạt động khung nào thường không kết hợp với những quá trình thiết kế giao diện người dùng
    1. Ước lượng giá
    2. Xây dựng giao diện
    3. Định trị giao diện
    4. Phân tích người dùng và tác vụ
13. Hướng tiếp cận nào để những phân tích tác vụ của người dùng trong thiết kế giao diện người dùng
    1. Người dùng cho biết những ưa thích qua bản câu hỏi
    2. Dựa vào ý kiến của những lập trình viên có kinh nghiệm
    3. Nghiên cứu những hệ thống tự động liên quan
    4. Quan sát thao tác người dùng
14. Những vấn đề thiết kế chung nổi trội lên trong hầu hết giao diện người dùng
    1. Kết nối tiền sử người dùng (profile) và shortcut chức năng
    2. Xử lý lỗi và thời gian đáp ứng của hệ thống
    3. Quyết định hiển thị hình ảnh và thiết kế icon
    4. Không có mục nào
15. Những hệ thống phát triển giao diện người dùng đặc trưng cung cấp những kỹ thuật cho việc xây dựng những nguyên mẫu giao diện bao gồm
    1. Tạo code
    2. Những tool vẽ
    3. Định trị input
    4. Tất cả mục trên
16. Những bản câu hỏi có ý nghĩa nhất đối với những người thiết kế giao diện khi được hoàn tất bởi
    1. Khách hàng
    2. Những lập trình viên có kinh nghiệm
    3. Người dùng sản phẩm
    4. Người quản lý dự án
17. Nhiều đo lường hữu dụng có thể thu thập khi quan sát những người dùng tương tác với hệ thống máy tính gồm
    1. Thời gian cho ứng dụng
    2. Số khiếm khuyết (defect) phần mềm
    3. Tính tin cậy của phần mềm
    4. Thời gian đọc tài liệu trợ giúp
18. Một bảng quyết định được dùng
    1. Để tư liệu tất cả những trạng thái phụ thuộc
    2. Để hướng dẫn phát triển kế hoạch quản lý dự án
    3. Chỉ khi xây dựng hệ chuyên gia
    4. Khi một tập phức tạp những điều kiện và hoạt động xuất hiện trong thành phần
19. Ngôn ngữ thiết kế chương trình (PDL) thường là một
    1. Sự kết hợp giữa cấu trúc lập trình và văn bản tường thuật
    2. Ngôn ngữ lập trình truyền thống theo luật riêng của nó
    3. Ngôn ngữ phát triển phần mềm có thể đọc bởi máy
    4. Một cách hữu dụng để biểu diễn kiến trúc phần mềm
20. Những độ đo phức tạp vòng (cyclomatic complexity metric) cung cấp cho người thiết kế thống tin về số
    1. Chu kỳ trong chương trình
    2. Số lỗi trong chương trình
    3. Những đường logic độc lập trong chương trình
    4. Những phát biểu của chương trình
21. Kiểm thử điều kiện là một kỹ thuật kiểm thử cấu trúc điều khiển mà những tiêu chuẩn dùng để thiết kế test-case
    1. Dựa vào kiểm thử đường cơ bản
    2. Thử thách điều kiện logic trong module phần mềm
    3. Chọn những đường dẫn kiểm tra dựa vào những vị trí và dùng những biến
    4. Tập trung vào việc kiểm thử việc giá trị những cấu trúc lặp
22. Kiểm thử luồng dữ liệu là một kỹ thuật kiểm thử cấu trúc điều khiển mà những tiêu chuẩn dùng để thiết kế test-case
    1. Dựa vào kiểm thử đường cơ bản
    2. Thử thách điều kiện logic trong module phần mềm
    3. Chọn những đường dẫn kiểm tra dựa vào những vị trí và dùng những biến
    4. Tập trung vào việc kiểm thử việc giá trị những cấu trúc lặp
23. Kiểm thử lặp là một kỹ thuật kiểm thử cấu trúc điều khiển mà những tiêu chuẩn dùng để thiết kế test-case
    1. Dựa vào kiểm thử đường cơ bản
    2. Thử thách điều kiện logic trong module phần mềm
    3. Chọn những đường dẫn kiểm tra dựa vào những vị trí và dùng những biến
    4. Tập trung vào việc kiểm thử việc giá trị những cấu trúc lặp
24. Kiểm thử Black-box cố gắng tìm ra những lỗi
    1. Chức năng không đầy đủ hay không đúng
    2. Những lỗi giao diện
    3. Những lỗi thực thi
    4. Tất cả mục trên
25. Lý do tốt nhất cho việc dùng nhóm kiểm tra phần mềm độc lập là
    1. Những người phát triển phần mềm không cần làm bất kỳ kiểm thử nào
    2. Những người lạ sẽ kiểm phần mềm rất chặt
    3. Những người kiểm thử không được dính dáng tới dự án cho đến khi kiểm thử bắt đầu
    4. Mâu thuẩn về quyền lợi giữa những người phát triển và những người kiểm thử sẽ giảm
26. Trong một dự án thành công sử dụng chiến lược
    1. Đưa ra những xem xét kỹ thuật hình thức ưu tiên trước khi kiểm thử
    2. Chỉ rõ những yêu cầu trong theo một cách thức có thể định lượng
    3. Quan tâm tới việc sử dụng những nhóm kiểm thử độc lập
    4. Tất cả mục trên
27. Kiểm thử tích hợp Top-down có thuận lợi chính là
    1. Những module mức thấp không bao giờ cần kiểm thử
    2. Những điểm quyết định chính được kiểm thử sớm
    3. Không có những stub cần phải viết
    4. Không có mục nào
28. Kiểm thử tích hợp bottom-up có những thuận lợi chính
    1. Những điểm quyết định chính được kiểm thử sớm
    2. Không có những driver cần được viết
    3. Không có những stub (nhánh) cần phải viết
    4. Không đòi hỏi kiểm thử hồi quy (regression)
29. Hướng debug
    1. Backtracking
    2. Brute force
    3. Sự loại trừ nguyên nhân
    4. Tất cả các mục
30. Những kiểm tra chấp nhận thường được đưa ra bởi
    1. Người phát triển
    2. Những người dùng cuối
    3. Nhóm kiểm thử
    4. Những kỹ sư hệ thống
31. Ai là người không thích hợp để tham dự vào nhóm FAST (facilitated application specification techniques)
    1. Kỹ sư phần cứng và phần mềm
    2. Đại diện nhà sản xuất
    3. Đại diện thị trường
    4. Nhân viên tài chánh cao cấp
32. Ba giai đoạn tổng quát của công nghệ phần mềm
    1. definition, development, support
    2. what, how, where
    3. programming, debugging, maintenance
    4. analysis, design, testing
33. Biểu đồ dịch chuyển trạng thái
    1. Đưa ra hình ảnh về các đối tượng dữ liệu
    2. Đưa ra hình ảnh chức năng biến đổi luồng dữ liệu
    3. Chỉ ra hình ảnh dữ liệu được biến đổi như thế nào bởi hệ thống
    4. Chỉ ra những tương tác của hệ thống đối với sự kiện bên ngoài
34. Biểu đồ dòng điều khiển
    1. Cần thiết để mô hình những hệ thống hướng sự kiện
    2. Được đòi hỏi cho tất cả hệ thống
    3. Được dùng trong biểu đồ dòng dữ liệu
    4. Hữu dụng trong mô hình hóa giao diện người dùng
35. Biểu đồ quan hệ thực thể
    1. Đưa ra hình ảnh quan hệ giữa các đối tượng dữ liệu
    2. Đưa ra hình ảnh những chức năng biến đổi luồng dữ liệu
    3. Chỉ ra những quyết định logic chính khi chúng xuất hiện
    4. Chỉ ra sự tương tác của hệ thống với sự kiện bên ngoài
36. Cách tốt nhất để đưa tới việc xem xét việc đánh giá yêu cầu là
    1. Kiểm tra lỗi mô hình hệ thống
    2. Nhờ khách hàng kiểm tra yêu cầu
    3. Gởi họ tới đội thiết kế và xem họ có sự quan tâm nào không
    4. Dùng danh sách các câu hỏi kiểm tra để kiểm tra mỗi yêu cầu
37. Cấp bậc điều khiển thể hiện
    1. Thứ tự quyết định
    2. Việc tổ chức của các module
    3. Sự lặp lại của những hoạt động
    4. Sự tuần tự của các tiến trình
38. Câu hỏi không được kỹ sư phần mềm hiện nay quan tâm nữa
    1. Tại sao chi phí phần cứng máy tính quá cao?
    2. Tại sao phần mềm mất một thời gian dài để hoàn tất?
    3. Tại sao người ta tốn nhiếu chi phí để phát triển một mẩu phần mềm?
    4. Tại sao những lỗi phần mềm không được loại bỏ trong sản phẩm trước khi xuất xưởng
39. Cấu trúc thông tin biểu diển tổ chức nội của
    1. Những cấu trúc dữ liệu dùng để biểu diễn loại dữ liệu
    2. Mô hình bố trí nhân viên dự án
    3. Mô hình truyền thông dự án
    4. Những dữ liệu khác nhau và những mục điều khiển
40. Chất lượng sản phẩm liên quan: product operation, product transition, product revision. Thuộc tính nào liên quan tới product revision:
    1. Reliability
    2. Maintainability
    3. Testability
    4. Portability
41. Chỉ phát biểu sai, bộ 3 ràng buộc
    1. Phạm vi
    2. Thời gian
    3. Chi phí
    4. Chất lượng
42. Chỉ phát biểu sai, các nhóm phần mềm (SUB-Team):
    1. Gồm một nhóm người
    2. Sub-Team System analysis có nhiệm vụ ước tính lợi nhuận
    3. Gồm một số người và nó phải tồn tại trong suốt dự án
    4. Có thể 1 người
43. Chỉ phát biểu sai, để đạt được độ đo PUM thấp:
    1. Cải tiến quy trình
    2. Giảm lỗi giá
    3. Gia tăng số bản bán được
    4. Giảm thời gian sửa lỗi
44. Chỉ phát biểu sai. Kiểm thử áp lực
    1. Thường áp dụng trong hệ thống phân bố
    2. Nếu quá tải thiết kế thì không cần xem xét tới lỗi hệ thống
    3. Có thể xem là một dạng của kiểm thử thực thi
    4. Thử thách dựa vào tải thiết kế cực đại
45. Chỉ phát biểu sai, lãnh vực hỗ trợ trong quản lý dự án
    1. Quản lý rủi ro
    2. Quản lý mua sắm
    3. Quản lý tích hợp
    4. Quản lý truyền thông
46. Chỉ phát biểu sai. Mô hình hướng ngắt
    1. Cho phép đáp ứng nhanh
    2. Dễ lập trình
    3. Ít gây ra xung đột
    4. Thường dùng trong hệ thống thời gian thực
47. Chỉ phát biểu sai. Phương pháp Brute Force
    1. “Để máy tính tìm ra lỗi”
    2. Gần giống với phương pháp “vét cạn”
    3. Là một phương pháp hiệu quả
    4. Thường lặp đi lặp lại thủ tục đơn giản nhiều lần
48. Chỉ phát biểu sai. Thiết kế dữ liệu ở mức thành phần:
    1. Thiết kế cơ sở dữ liệu
    2. Hiện thực thuộc tính dữ liệu thành cấu trúc dữ liệu
    3. Phát triển một tập những trừu tượng dữ liệu
    4. Tinh chế các đối tượng dữ liệu
49. Chỉ phát biểu sai. V & V (Verification and Validation)
    1. Đánh giá hệ thống có tính sử dụng hay không
    2. Liên quan tới vấn đề debug và bảo mật
    3. Nó và kiểm thử là hai lãnh vực riêng
    4. Nhằm kiểm tra phần mềm phải thực hiện những gì người dùng thực sự cần
50. Chỉ ra mục sai. Trong mô hình WebE trong mô hình phân tích có
    1. Phân tích nội dung
    2. Phân tích cấu hình
    3. Phân tích tương tác
    4. Phân tích điều hướng (naviation)
51. Để biết được địa chỉ IP cổng Internet bạn đang dùng có nằm trong danh sách nạn nhân của các chiến dịch tấn công mạng, botnet... trong 30 ngày gần nhất. Bạn sẽ vào đâu để kiểm tra nhanh nhất?
    1. <https://ais.gov.vn>
    2. <https://khonggianmang.vn>
    3. <http://antoanthongtin.vn>
    4. <http://vncert.gov.vn>
52. Theo bạn, đâu là công cụ kiểm tra trực tuyến địa chỉ website mà bạn nhập vào có phải là website lừa đảo hay không?
    1. https://khonggianmang.vn/check-phishing
    2. <http://antoanthongtin.vn>/check-phishing
    3. <http://vncert.gov.vn>/check-phishing
    4. <https://ais.gov.vn>/check-phishing
53. Để kiểm tra địa chỉ email của bạn có bị lộ lọt thông tin tài khoản không, bạn sẽ truy cập vào đâu để thực hiện điều này?
    1. <https://khonggianmang.vn/check-data-leak>
    2. Trang thông tin điện tử của Trung tâm giám sát an toàn không gian mạng quốc gia
    3. Website của nhà mạng
    4. Cả A và B đều được.
54. Khi duyệt web, nếu người dùng gặp phải lỗi như hình dưới đây, theo bạn đó là lỗi gì?



* 1. Máy tính người dùng đang sử dụng phiên bản Windows 7
  2. Chứng chỉ bảo mật SSL hết hạn hoặc không tin cậy
  3. Máy tính người dùng bị mã độc tấn công
  4. Cả A và B đúng

1. Trong thời gian vừa qua, tại sao phần mềm họp trực tuyến Zoom không được khuyến nghị sử dụng?
   1. Việc sử dụng phần mềm này khó do chưa hỗ trợ ngôn ngữ tiếng Việt
   2. Phần mềm này tồn tại một số lỗ hổng bảo mật nghiêm trọng như: mã hóa dữ liệu đầu cuối kém, dễ dàng bị dò quét ID cuộc họp, lỗ hổng liên quan đến đường dẫn UNC
   3. Cả B và D đúng
   4. Nhiều lỗ hổng bảo mật của Zoom đã được công bố mã lỗ hổng nhưng nhà cung cấp chưa xử lý triệt để
2. Theo bạn, đâu không phải là nhóm APT có mục tiêu tấn công vào Việt Nam theo thông tin cung cấp từ Cục An toàn thông tin – Bộ TT&TT?
   1. Goblin Panda
   2. Blackping
   3. Mustang Panda
   4. Gothic Panda
3. Theo bạn, đâu là mã lỗ hổng trong Microsoft Office cho phép chèn và thực thi mã lệnh?
   1. Tất cả B, C, D đều đúng
   2. CVE-2017-11882
   3. CVE-2018-0802
   4. CVE-2017-0199
4. Theo bạn, đâu là thư mục chứa các thư được coi là rác trên hệ thống thư điện tử công vụ của tỉnh?
   1. Spam
   2. Email Rác
   3. Junk E-mail
   4. Tất cả các đáp án trên
5. Theo bạn, đâu là thư mục chứa các thư được coi là rác trên hệ thống thư điện tử công vụ của tỉnh?
   1. Spam email
   2. Drafts
   3. Đáp án A, D đúng
   4. Junk E-mail
6. Bạn hoặc người dùng tại cơ quan/đơn vị/địa phương bạn nhận được thư có nội dung như mô tả trong hình dưới đây, theo bạn nội dung thư nói về điều gì?

Ảnh có chứa bàn

Mô tả được tạo tự động

* 1. Có 6 thư rác đã từng được gửi tới hộp thư của người dùng
  2. Có 6 thư rác đã từng được gửi vào hộp thư của người dùng và có trong thư mục Email Rác
  3. Có 6 thư rác đã từng được gửi tới hộp thư của người dùng nhưng được hệ thống chặn lại
  4. Đáp án A, C

1. Bạn hoặc người dùng tại cơ quan/đơn vị/địa phương bạn nhận được thư có nội dung như mô tả trong hình dưới đây, theo bạn đâu là đáp án đúng nhất?

Ảnh có chứa bàn

Mô tả được tạo tự động

* 1. Có 6 thư rác đã được gửi tới hộp thư của người dùng nhưng chưa được lưu vào bất kỳ thư mục nào trong hộp thư
  2. Có 6 thư rác được cách ly và đưa vào thư mục Email Rác
  3. Có 6 thư rác đã từng được gửi tới hộp thư của người dùng nhưng được hệ thống cách ly, người dùng có thể lựa chọn cho vào hoặc yêu cầu hệ thống xóa.
  4. Có 6 thư nghi nhiễm mã độc đã được hệ thống cách ly

1. Theo bạn, đâu là địa chỉ hộp thư tự động của hệ thống thư công vụ tỉnh Lào Cai gửi báo cáo hàng tuần về những thư nghi là thư rác được gửi tới hộp thư của người dùng?
   1. release-ctrl@fm400e.laocai.gov.vn
   2. release-ctrl@laocai.gov.vn
   3. hotro@.laocai.gov.vn
   4. release-ctrl@fm400d.laocai.gov.vn
2. Theo bạn, đâu là dải địa chỉ Private cấp phát trên hệ thống mạng thông tin của tỉnh?
   1. 10.118.1.0/16
   2. 10.118.0.0/16
   3. 10.118.0.0/24
   4. 10.118.0.0/32
3. Bạn muốn kiểm tra địa chỉ IP public của cổng Internet của cơ quan mình, Website nào dưới đây cung cấp công cụ giúp bạn thực hiện điều đó?
   1. www.showmyip.com
   2. khonggianmang.vn
   3. sotttt.laocai.gov.vn
   4. Đáp án A và B
4. Theo bạn, đâu là những đặc trưng cơ bản của chữ ký số?
   1. Xác thực, toàn vẹn, bí mật, chống chối bỏ
   2. Xác thực, định danh, toàn vẹn, chống chối bỏ
   3. Xác thực, an toàn, bí mật, chống chối bỏ
   4. Xác thực, định danh, bí mật, chống chối bỏ
5. Khi văn bản đã được ký số, theo bạn phát biểu nào sau đây là đúng nhất?
   1. Có thể xác định được thông tin người ký văn bản
   2. Có thể sửa được nội dung văn bản
   3. Xác định được chi tiết thông tin về thời gian: ngày, giờ, phút, giây ký số
   4. Xác định được địa điểm ký văn bản
6. Theo bạn phát biểu nào sau đây là đúng khi nói về chữ ký số?
   1. Có thể ký số trên văn bản giấy
   2. Có thể ký số trên tệp tin Microsoft Powerpoint
   3. B, D đều đúng
   4. Chỉ có thể ký số trên những loại tệp tin được truyền, đưa trên môi trường mạng
7. Theo bạn phát biểu nào sau đây là sai khi nói về chữ ký số?
   1. Không có chứng thư số cho thiết bị, dịch vụ, phần mềm
   2. Có chứng thư số cho cá nhân
   3. Có chứng thư số cho cá nhân, cơ quan, tổ chức
   4. Đáp án B, C đúng
8. Trong mạng LAN của đơn vị bạn có một số máy tính bị nhiễm mã độc làm cho việc truy cập Internet của các máy tính khác trong mạng chậm một cách bất thường, bằng cách nào nhanh nhất tìm ra máy tính nghi ngờ bị nhiễm mã độc?
   1. Cài đặt ngay phần mềm rà quét lỗ hổng bảo mật
   2. Ngắt kết nối mạng LAN với Internet
   3. Quan sát trạng thái đèn chỉ thị trên các cổng Switch
   4. Quan sát trạng thái đèn chỉ thị trên Router Internet
9. Khi người dùng tại cơ quan/đơn vị/địa phương bạn truy cập vào các phần mềm dùng chung của tỉnh đều bị chậm, theo bạn nguyên nhân thường do đâu?
   1. Máy chủ cài đặt phần mềm dùng chung của tỉnh có cấu hình thấp
   2. Cổng Internet phía các máy chủ cài đặt phần mềm dùng chung có băng thông thấp
   3. Băng thông Internet phía người dùng có thể bị nghẽn
   4. Đáp án A, B
10. Bạn muốn kiểm tra tệp tin nghi nhiễm mã độc, website nào sau đây giúp bạn thực hiện nhanh điều đó?
    1. https://www.virustotal.com
    2. https://virus.com
    3. https://khonggianmang.vn
    4. https://bkav.vn
11. Theo bạn, đâu là phần mềm hiện không còn được nhà cung cấp hỗ trợ cập nhật bản vá bảo mật?
    1. Microsoft Windows 7
    2. Microsoft Windows Server 2008 R2
    3. Microsoft Office 2007
    4. Tất cả các đáp án A, B, C đều đúng
12. Theo bạn, đâu là phần mềm hiện không còn được nhà cung cấp hỗ trợ cập nhật bản vá bảo mật?
    1. Đáp án B, C đúng
    2. Microsoft SQL Server 2008
    3. Microsoft Internet Explorer 10
    4. Microsoft Office 2010
13. Tính đến thời điểm 10/5/2020, theo bạn đâu là phiên bản hệ điều hành mới nhất?
    1. Ubuntu Ubuntu 20.04 LTS
    2. Microsoft Windows Server 2020
    3. Microsoft Windows 10 version 1903
    4. Tất cả các đáp án trên
14. Tính đến thời điểm 10/5/2020, theo bạn đâu là phiên bản hệ điều hành mới nhất?
    1. Ubuntu Ubuntu 20.05 LTS
    2. Microsoft Windows Server 2020
    3. Microsoft Windows 10 version 1909
    4. Tất cả các đáp án trên
15. Để nâng cao công tác bảo đảm an toàn thông tin, bạn được cơ quan giao nhiệm vụ đề xuất lựa chọn mua sắm phần mềm Microsoft Office bảo đảm đến năm 2021 vẫn được hãng hỗ trợ cập nhật bản vá, bạn sẽ lựa chọn phần mềm phiên bản nào dưới đây?
    1. Microsoft Office 2010
    2. Microsoft Office 2020
    3. Microsoft Office 365
    4. Có thể lựa chọn B và C
16. Để nâng cao công tác bảo đảm an toàn thông tin, bạn được cơ quan giao nhiệm vụ đề xuất lựa chọn mua sắm phần mềm Microsoft windows cho máy tính cá nhân bảo đảm đến năm 2021 vẫn được hãng hỗ trợ cập nhật bản vá, bạn sẽ lựa chọn phiên bản nào dưới đây?
    1. Windows 10 version 1803 Pro
    2. Windows Thin PC
    3. Windows 10 version 1909
    4. Windows 10 Enterprise 2016 LTSB
17. Để thực hiện việc cập nhật bản vá cho các máy chủ đặt trong vùng không được phép kết nối trực tiếp với Internet, bạn sẽ lựa chọn giải pháp nào sau đây?
    1. Sử dụng phần mềm WSUS Offline Update
    2. Sử dụng phần mềm Windows Server Update Services (WSUS)
    3. Sử dụng phần mềm Windows Server
    4. Có thể sử dụng giải pháp A hoặc B
18. Theo bạn, trong vai trò là cán bộ chuyên trách CNTT/ATTT của cơ quan, trước khi đề xuất việc nâng cấp, trang bị các giải pháp bảo đảm an toàn cho hệ thống mạng của cơ quan/đơn vị/địa phương mình, cơ quan bạn cần thực hiện việc gì trước tiên?
    1. Khảo sát hiện trạng, xây dựng giải pháp
    2. Xây dựng, trình phê duyệt hồ sơ cấp độ hệ thống thông tin
    3. Khảo sát hiện trạng, xác định nhu cầu
    4. Khảo sát hiện trạng
19. Giả sử tại cơ quan/đơn vị/địa phương nơi bạn công tác đều sử dụng hệ điều hành Microsoft windows, để kiểm soát toàn diện người dùng, nâng cao hiệu quả bảo đảm an toàn thông tin, theo bạn sử dụng giải pháp nào sau đây để đáp ứng yêu cầu?
    1. Triển khai Domain Controller
    2. Triển khai giải pháp Antivirus tập trung
    3. Triển khai thiết bị tường lửa chuyên dùng
    4. Triển khai phần mềm tường lửa
20. Trường khóa chính là trường:
    1. Single Key
    2. Unique Key
    3. First Key
    4. Primary Key
21. Câu nào trong các câu dưới đây sai khi nói về hệ CSDL khách-chủ?
    1. Trong kiến trúc khách-chủ, các thành phần (của hệ QTCSDL) tương tác với nhau tạo nên hệ thống gồm thành phần yêu cầu tài nguyên và thành phần cấp tài nguyên
    2. Hai thành phần yêu cầu tài nguyên và thành phần cấp tài nguyên phải cài đặt trên cùng một máy tính
    3. Thành phần cấp tài nguyên thường được cài đặt tại một máy chủ trên mạng (cục bộ)
    4. Thành phần yêu cầu tài nguyên có thể cài đặt tại nhiều máy khác (máy khách) trên mạng
22. Hãy chọn phương án đúng. Hai bảng trong một CSDL quan hệ liên kết với nhau thông qua:

A. Địa chỉ của các bảng

B. Tên trường

C. Thuộc tính của các trường được chọn (không nhất thiết phải là khóa)

D. Thuộc tính khóa

1. Câu nào trong các câu dưới đây sai khi nói về hệ CSDL cá nhân?

A. Người dùng đóng vai trò là người quản trị CSDL

B. Tính an toàn của hệ CSDL cá nhân rất cao

C. Hệ CSDL cá nhân được lưu trữ trên 1 máy

D. Hệ CSDL chỉ cho phép 1 người dùng tại một thời điểm

1. Tiêu chí nào sau đây thường được dùng để chọn khóa chính?

A. Khóa có ít thuộc tính nhất

B. Không chứa các thuộc tính thay đổi theo thời gian

C. Khóa bất kì

D. Chỉ là khóa có một thuộc tính

1. Thế nào là cơ sở dữ liệu quan hệ?

A. Cơ sở dữ liệu được xây dựng dựa trên mô hình dữ liệu quan hệ

B. Cơ sở dữ liệu dùng để tạo lập, cập nhật và khai thác CSDL quan hệ

C. Cơ sở dữ liệu được xây dựng dựa trên mô hình dữ liệu quan hệ và khai thác

CSDL quan hệ

D. Cơ sở dữ liệu dùng để tạo lập, cập nhật và khai thác CSDL quan hệ dựa trên mô hình dữ liệu quan hệ

1. Liên kết giữa các bảng được dựa trên:

A. Thuộc tính khóa

B. Các thuộc tính trùng tên nhau giữa các bảng

C. Ý định của người quản trị hệ CSDL

D. Ý định ghép các bảng thành một bảng có nhiều thuộc tính hơn

1. Câu nào sai trong các câu dưới đây khi nói về ưu điểm của hệ CSDL khách-chủ?

A. Chi phí cho truyền thông giảm

B. Bổ sung thêm máy khách là dễ dàng

C. Phát triển và sử dụng các hệ CSDL khách-chủ khá đơn giản, dễ dàng

D. Nâng cao khả năng đảm bảo tính nhất quán của dữ liệu

1. Khẳng định nào sau đây về CSDL quan hệ là đúng?

A. Tập hợp các bảng dữ liệu

B. Cơ sở dữ liệu được tạo ra từ hệ QTCSDL Access

C. Cơ sở dữ liệu mà giữa các dữ liệu có quan hệ với nhau

D. Cơ sở dữ liệu được xây dựng trên mô hình dữ liệu quan hệ

1. Câu nào sai trong các câu dưới đây?

A. Mỗi bảng có ít nhất một khóa

B. Nên chọn khóa chính là khóa có ít thuộc tính nhất

C. Trong một bảng có thể có nhiều khóa chính

D. Việc xác định khóa phụ thuộc vào quan hệ logic của các dữ liệu chứ không phụ thuộc vào giá trị các dữ liệu

1. Trong quá trình cập nhật dữ liệu, được hệ quản trị CSDL kiểm soát để đảm bảo tính chất nào?

A. Tính chất ràng buộc toàn vẹn

B. Tính độc lập

C. Tính nhất quán

D. Tính bảo mật

1. Hãy cho biết ý kiến nào là đúng. Với một bảng dữ liệu, hệ QTCSDL cho phép:

A. Xem nội dung các bản ghi

B. Xem mối liên kết giữa bảng đó với các bảng khác

C. Xem một số trường của mỗi bản ghi

D. Tất cả đều đúng

1. Câu nào trong các câu dưới đây sai khi nói về hệ CSDL trung tâm?

A. Là hệ CSDL được cài đặt trên máy tính trung tâm cho phép nhiều người sử dụng cùng một lúc

B. Máy tính trung tâm này chỉ là một máy tính duy nhất

C. Nhiều người dùng từ xa có thể truy cập vào CSDL này thông qua thiết bị đầu

cuối và các phương tiện truyền thông

D. Các hệ CSDL trung tâm thường rất lớn và có nhiều người dùng

1. Trong các ưu điểm dưới đây, ưu điểm nào không phải của các hệ CSDL phân tán?

A. Dữ liệu có tính sẵn sàng

B. Dữ liệu được chia sẻ trên mạng nhưng vẫn cho phép quản trị dữ liệu địa phương

C. Việc thiết kế CSDL đơn giản, chi phí thấp hơn

D. Dữ liệu có tính tin cậy cao

1. Câu nào sai trong các câu dưới đây khi nói về ưu điểm của hệ CSDL khách-chủ?

A. Khả năng truy cập rộng rãi đến các CSDL

B. Phát triển và sử dụng các hệ CSDL khách-chủ khá đơn giản, dễ dàng

C. Nâng cao khả năng thực hiện

D. Chi phí cho phần cứng có thể giảm

1. Trong các phần mềm sau đây, phần mềm nào không phải là hệ quản trị CSDL quan hệ?

A. Microsoft Excel

B. Microsoft Access

C. Microsoft SQL server

D. Oracle

1. Đâu không phải là các bước xây dựng cơ sở dữ liệu?

A. Thiết kế

B. Khảo sát

C. Chạy thử

D. Ký hợp đồng

1. Hãy chọn phương án trả lời đúng. Có các câu trả lời sau cho câu hỏi : "Tại sao phải khai báo kích thước cho mỗi trường?"

A. Để giúp hệ thống kiểm tra tính đúng đắn khi nhập dữ liệu

B. Để có thể tính kích thước của bản ghi (bộ dữ liệu) và xác định vị trí các trường trong bản ghi

C. Để hệ thống dự trữ vùng nhớ phục vụ ghi dữ liệu

D. Tất cả đều đúng

1. Các bước chính để tạo CSDL:

A. Tạo bảng; Chọn khóa chính cho bảng; Đặt tên bảng và lưu cấu trúc bảng; Tạo liên kết bảng

B. Tạo bảng; Chọn khóa chính cho bảng; Đặt tên bảng và lưu cấu trúc bảng

C. Tạo bảng; Chọn khóa chính cho bảng; Lưu cấu trúc bảng; Tạo liên kết bảng; cập nhật và khai thác CSDL

D. Tạo bảng; Chọn khóa chính cho bảng; Đặt tên bảng; Tạo liên kết bảng

1. SQL là tên viết tắt của:

A. Structure Query Language

B. Query Structure Language

C. Structure Question Language

D. Structure Query Locator

1. An toàn dữ liệu có thể hiểu là?

A. Dễ dàng cho công việc bảo trì dữ liệu

B. Ngăn chặn các truy nhập trái phép, sai quy định từ trong ra hoặc từ ngoài vào

C. Thống nhất các tiêu chuẩn, thủ tục và các biện pháp bảo vệ, an toàn dữ liệu

D. Tính nhất quán và toàn vẹn dữ liệu

1. Mô hình ngoài là?

A. Nội dung thông tin của toàn bộ CSDL

B. Nội dung thông tin của toàn bộ CSDL dưới cách nhìn của người sử dụng

C. Nội dung thông tin của một phần cơ sở dữ liệu

D. Nội dung thông tin của một phần dữ liệu dưới cách nhìn của người sử dụng

1. Mô hình trong là?

A. Là một trong các mô hình biểu diễn CSDL dưới dạng lưu trữ vật lý

B. Mô hình biểu diễn cơ sở dữ liệu trìu tượng ở mức quan niệm

C. Có nhiều cách biểu diễn CSDL dưới dạng lưu trữ vật lý

D. Mô hình lưu trữ vật lý dữ liệu

1. Ánh xạ quan niệm-ngoài?

A. Quan hệ giữa mô hình trong và mô hình trong

B. Quan hệ giữa mô hình ngoài và mô hình ngoài

C. Quan hệ giữa mô hình ngoài và mô hình trong

D. Quan hệ môt-một giữa mô hình ngoài và mô hình dữ liệu

1. Mục tiêu của cơ sở dữ liệu là?

A. Không làm thay đổi chiến lược truy nhập cơ sở dữ liệu

B. Bảo đảm tính độc lập dữ liệu

C. Không làm thay đổi cấu trúc lưu trữ dữ liệu

D. Dữ liệu chỉ được biểu diễn, mô tả một cách duy nhất

1. Ràng buộc giải tích?

A. Quy tắc biểu diễn cấu trúc dữ liệu

B. Mối quan hệ giữa các thuộc tính được biểu diễn bằng các biểu thức toán học

C. Mô tả tính chất của các thuộc tính khi tạo lập CSDL

D. Các phép toán đại số quan hệ

1. Ràng buộc logic?

A. Mối quan hệ giữa các thuộc tính được biểu diễn bằng các phụ thuộc hàm

B. Mối quan hệ giữa các thuộc tính được biểu diễn bằng các biểu thức toán học

C. Các phép so sánh

D. Các phép toán quan hệ

1. Mô hình CSDL phân cấp là mô hình?

A. Dữ liệu được biểu diễn bằng con trỏ

B. Dữ liệu được biểu diễn bằng mối quan hệ thực thể

C. Dữ liệu được biểu diễn bằng bảng

D. Dữ liệu được biểu diễn bằng cấu trúc cây

1. Khi thao tác bằng ngôn ngữ thao tác dữ liệu trên CSDL phân cấp?

A. Đảm bảo tính độc lập của dữ liệu

B. Đảm bảo tính ổn định

C. Đảm bảo tính toàn vẹn của dữ liệu

D. Có nhiều khả năng xẩy ra di thường thông tin

1. Đặc trưng cấu trúc của mô hình mạng là?

A. Chứa các liên kết một - một và một - nhiều

B. Chứa các liên kết một - một, một - nhiều và nhiều - nhiều

C. Chứa các liên kết một - một, một - nhiều và nhiều - nhiều

D. Chứa các liên kết nhiều - một và một - nhiều

1. Yêu cầu  để đảm bảo sử dụng mã  hóa đối xứng là
   1. 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
   2. Có một kênh truyền phù hợp và một khóa bí mật được biết bởi người nhận/gởi
   3. Có thuật tóan encryption tốt và có một khóa bí mật được biết bởi người nhận/gởi
   4. Tất cả đều đúng
2. Các thuật tóan nào sau đây là thuật tóan mã  hóa đối xứng
   1. Triple –DES, RC4, RC5, Blowfish
   2. Triple –DES, RC4, RC5, IDEA
   3. RC4, RC5, IDEA, Blowfish
   4. IDEA, Blowfish, AES, Elliptic Cure
3. Các phát biểu sau đây phát biểu nào đúng
   1. Hầu hết các thuật tóan mã hóa đối xứng đều dựa trên cấu trúc thuật tóan Feistel
   2. Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa
   3. Hầu hết các thuật tóan mã hóa khối đều đối xứng
   4. Tất cả đều đúng
4. Cơ  chế bảo mật SSL hoạt  động trên tầng
   1. Network, Transport
   2. Network, Session
   3. Application, Session
   4. Tất cả đều sai
5. Keberos là  dịch vụ ủy thác
   1. Xác thực trên Web
   2. Xác thực X.509
   3. Xác thực trên Server
   4. Xác thực trên các máy trạm với nhau
6. PGP là  giao thức để xác thực
   1. Quyền đăng cập vào hệ thống máy chủ Window
   2. Bảo mật cho thư  điện tử
   3. Thực hiện mã hóa thông điệp theo thuật tóan RSA
   4. Địa chỉ của máy trạm khi kết nối vào Internet
7. Công cụ/cơ  chế  bảo mật cho mạng không dây là
   1. SSL
   2. TSL
   3. Giao thức PGP
   4. WEP
8. Giao thứ  SSL và TSL hoạt động ở tầng nào của mô  hình OSI
   1. Network
   2. Sesion
   3. Transport
   4. Từ tầng Trasport trở lên
9. Giao thức SSL dùng để
   1. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP
   2. Cung cấp bảo mật cho thư điện tử
   3. Cung cấp bảo mật cho Web
   4. 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
    1. Lây nhiễm và sinh sản
    2. Sống ký sinh và  lây nhiễm
    3. Tự phát triển  độc lập và lây nhiễm
    4. Tất cả đều đúng
11. Hoạt  động của virus có 4 giai đoạn
    1. Nằm im, lây nhiễm, tàn phá và tự hủy
    2. Lây nhiễm, tấn công, hủy diệt và tự hủy
    3. Nằm im, lây nhiễm, khởi sự và tàn phá
    4. Lây nhiễm, khởi sự, tàn phát, kích họat lại
12. Các dạng sau đây, dạng nào là của virus
    1. sealth, cư trú  bộ nhớ, macro, đa hình, file
    2. stealth, cư trú  bộ nhớ, macro, lưỡng tính, file
    3. virus ký sinh, file, boot secctor, stealth, cư trú bộ nhớ, macro
    4. 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
    1. MS.Exel, MX Word, MS.Outlook Mail
    2. MS.Exel, MX Word, MS.Power Point
    3. MS.Exel, MX Word,Yahoo Mail
    4. 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
    1. Tầng Network
    2. Tầng Transport
    3. Từ tầng Transport trở lên đến tầng 7
    4. Tầng Session
15. Kỹ  thuật tấn công phổ biến trên Web là
    1. Chiếm hữu phiên làm việc.
    2. Tràn bộ đệm.
    3. Từ chối dịch vụ (DoS)
    4. Chèn câu truy vấn SQL.
16. Các lỗ  hổng bảo mật trên hệ  thống là do
    1. Dịch vụ cung cấp
    2. Bản thân hệ điều hành
    3. Con người tạo ra
    4. Tất cả đều đúng
17. Cho biết câu nào  đúng trong các câu sau
    1. 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
    2. 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
    3. Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm
    4. Tất cả đều đúng
18. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên ( session) của mô  hình OSI
    1. Packet filtering firewall
    2. Circuit level firewall
    3. Application level firewall
    4. 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)
    1. PPP
    2. ATM
    3. HDLC
    4. SDLC
20. Khi thuê một giải pháp VPN, những loại tấn công nào bạn cần phải xét đến ?
    1. Denial of Service (DoS) attacks, Internet Viruses.
    2. Distributed Denial of Service (DDoS) attacks.
    3. Data confidentiality, IP Spoofing.
    4. Network mapping, Internet Viruses.
21. Các phát biểu sau đây phát biểu là là  đúng nhất
    1. Fire wal là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công
    2. Là một điểm chặn của trong quá trình điều khiển và giám sát.
    3. Là một phần mềm hoặc phần ứng có khả năng ngăn chặn tấn công từ bên trong và bên ngoài vào hệ thống.
    4. 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
    1. Tính tin cẩn (confidentiality), Tính xác nhận, Toàn vẹn thông điệp (integrity), Sự thối thác ban đầu (non-repudiation of origin)
    2. Tính xác nhận,Toàn vẹn thông điệp(integrity), Sự thối thác ban đầu (non-repudiation of origin), tính bền vững
    3. Sự thối thác ban đầu (non-repudiation of origin), tính bền vững, tính ổn khi gởi và nhận
    4. Tất cả đều đúng
23. Các giao thức  được để bảo mật thư  điện tử là
    1. GPG, S/MINE
    2. SHA-1, S/MINE
    3. CAST-128 / IDEA/3DES
    4. Keboros, X.509
24. Chữ ký điện tử (digital signature) sử dụng thuật tóan nào sau đây
    1. RSA,MD5
    2. RSA,MD5, Keboros
    3. MD5, SHA,RSA
    4. Không dùng thuật tóan nào nêu trên
25. Chữ  ký điện tử là
    1. Là một chuỗi đã được mã hóa theo thuật tóan băm và đính kèm với văn bản gốc trước khi gởi.
    2. 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.
    3. a và b đều đúng
    4. Tất cả cả  đều sai
26. Các bước mã  hóa của chứ ký điện tử
    1. 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.
    2. 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.
    3. 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.
    4. Tất cả đều đúng
27. Các bước kiểm tra của chứ ký điện tử
    1. 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.
    2. Chỉ có bước 1 và 2
    3. 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
    4. 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
    1. RSA
    2. Keberos
    3. MD5
    4. SHA
29. Để thực hiện tấn công bằng Trojan, kẻ  tấn công chỉ cần
    1. Tạo 1 file chạy (\*.exe, \*.com) vận hành trên máy nạn nhân là đủ
    2. Cho máy nạn nhân lây nhiễm một loại virus bất kỳ nào đó.
    3. Thực hiện đồng thời 2 file, một file vận hành trên máy nạn nhân, file còn lại họat động điều khiển trên máy kẻ tấn công.
    4. Không có điều nào đúng.
30. Giao thức bảo mật IPSec họat động ở tầng
    1. Chỉ ở tầng transport ở mô hình OSI
    2. Từ tầng 4 tới tầng 7 ở mô hình OSI
    3. Network Layer ở mô hình OSI
    4. Tất cả đều sai
31. Cho biết phát biểu sau đây phát biểu nào là  đúng nhất về registry
    1. 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.
    2. Regỉstry là một phần mềm tiện ích hỗ trợ cho người dùng thay đổi cấu hình Window khi cần thiết
    3. Registry là một thành phần của hệ điều hành Window
    4. Tất cả đều đúng
32. Có  bao nhiêu kiểu dữ liệu trong Registry
    1. 5
    2. 4
    3. 6
    4. 7
33. Các kiểu dữ  liệu dùng trong registry là
    1. interger, real,text,string
    2. HKEY\_CLASSES\_ROOT, -USER, HKEY\_LOCAL\_MACHINE, HKEY\_USERS, HKEY\_CURRENT\_CONFIG, HKEY\_DYN\_DATA
    3. HKEY\_CLASSES\_ROOT, -USER, HKEY\_LOCAL\_MACHINE, REG\_BINARY
    4. 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
    1. 65656000
    2. 67188270
    3. 67108863
    4. Tất cả đều sai
35. Để sử dụng xác thực Keberos V5 ở tất cả máy trạm Window98, người ta thực hiện :
    1. Update window 98 lên XP hoặc Window 2000
    2. Cài đặt tiện  ích Distributed Security Client trên tất cả các máy chạy Window 98
    3. Chỉ cần cài  đặt Active Directory trên Server hệ thống
    4. 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 ?
    1. Update Window 2000 mà  không remote trước khi cài đặt
    2. Cài đặt Window 2000  nhiều lần trên Server
    3. Bản Window 2000 không có bản quyền
    4. Tất cả đều đúng
37. Dịch vụ  Active Directory thực hiện các chức năng sau
    1. Tổ chức và  xây dựng các domain; xác thực và cấp quyền cho các  đối tượng
    2. Duy các hoạt động của các dịch vụ bảo mật cho Window Server và xác thực, cấp quyền cho các đối tượng
    3. Chỉ thực hiện việc xác thực và cấp các quyền cho users và groups
    4. Quản lý tài nguyên và người dùng; xác thực và cấp các quyền cho users và groups; giám sát họat động của các user
38. Thuật tóan thực hiện trong cơ chế bảo mật IP (IP Sec) ở Window sử dụng là
    1. MD5 và SHA1
    2. Kerberos và DES
    3. DES hoặc 3DES (triple DES).
    4. Tất cả đều sai
39. Trong Window 98,XP Registry được lưu trữ ở đâu ?
    1. Được lưu trong file Classes.dat trong thư mục Windows
    2. Được lưu trong thư  mục "Windows System32 Config
    3. Trong 2 file: user.dat và system.dat trong thư mục Windows
    4. Tất cả đều sai
40. Để thực hiện sửa đổi cấu hình trên registry ta thực hiện như sau:
    1. Gõ regedit vào cửa sổ Run
    2. Bấm Ctrl+ Esc+ r  rồi bấm Enter
    3. a và b đúng
    4. Tất cả đều sai
41. Quy trình crack một sản phẩm phần mềm đơn giản gồm mấy bước
    1. 3
    2. 4
    3. 5
    4. 3 hoặc 4
42. Hai giao thức  sử dụng trong IPSec (IPSec Protocol) gồm
    1. IP Authentication Header, TCP/IP
    2. TCP/IP, IP Encapsulating Security Payload
    3. IP Authentication Header, IP Encapsulating Security Payload
    4. Tất cả đều đúng
43. Các  điểm khác nhau cơ bản giữa dịch vụ  X.509 và Kerberos là
    1. Dựa trên mã hóa  đối xứng
    2. Được sử dụng trong dịch vụ mail
    3. Xác thực nhiều chiều
    4. Tất cả đều đúng
44. Các chức năng cơ bản của kỹ thuật tấn công Sniffer
    1. 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.
    2. Bắt gói tin trên  đường truyền, phân tích lỗi và giải mã gói tin
    3. Bắt gói tin trên  đường truyền, mã hóa vag giải mã dữ liệu
    4. Tất cả đều đúng
45. Các bước tấn công của Web Server theo trình tự  sau :
    1. Thăm dò, Scan, Giành quyền truy cập, Duy trì truy cập, Xóa vết
    2. Scan, Thăm dò, Giành quyền truy cập, Duy trì truy cập, Xóa vết
    3. Thăm dò, Scan, Duy trì  truy cập, Giành quyền truy cập, Xóa vết
    4. 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…
    1. Virrus,Zombie
    2. Worm, Virus
    3. Logicbomb, Virus
    4. Trapdoors, Trojan
47. Để  đánh giá điểm mạnh của hệ  thống IDS người ta dựa vào các yếu tố  sau :
    1. Khởi sự, Cách thực hiện, biểu hiện mà nó ghi nhận
    2. Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp
    3. Cách thực hiện, biểu hiện mà nó ghi nhận, những đặc trưng ghép nối hoặc tích hợp
    4. 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 :
    1. Phát hiện biểu hiện không bình thường, phát hiện sử dụng không đúng
    2. Phát hiện hiện tượng trùng lặp, phát hiện không bình thường
    3. Phát hiện thay đổi, phát hiện sử dụng bất bình thường
    4. Tất cả đều đúng
49. Mục tiêu là phân tích mật mã là gì?
    1. Để xác định thế mạnh của các thuật toán một
    2. Để tăng cường chức năng thay thế trong một thuật toán mật mã
    3. Để giảm chức năng transposition trong một thuật toán mật mã
    4. Để xác định hoán vị sử dụng
50. Điều gì sẽ xãy ra khi một thông báo đã được sửa đổi?
    1. Khoá công cộng đã được thay đổi
    2. Chìa khóa cá nhân đã được thay đổi
    3. Thông điệp số đã được thay đổi
    4. 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?
    1. Data Encryption Standard
    2. Digital Signature Standard
    3. Secure Hash Algorithm
    4. 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?
    1. Tấn công Man-in-the-middle
    2. Tấn công Birthday
    3. Tấn công Denial of Service
    4. Tấn công Dictionary
53. Lợi thế của RSA là gì so với DSS?
    1. Nó có thể cung cấp cho chữ ký số và mã hóa các chức năng
    2. Nó sử dụng nguồn tài nguyên ít hơn và mã hóa nhanh hơn bởi vì nó sử dụng các phím đối xứng
    3. Nó là một thuật toán mật mã khối so với một thuật toán mật mã dòng
    4. Nó sử dụng một lần mã hóa pad
54. Những gì  được sử dụng để tạo ra một chữ  ký điện tử?
    1. Khóa riêng của người nhận
    2. Khóa công khai của người gửi
    3. Khóa riêng của người gửi
    4. Khóa công khai của người nhận
55. Phương thức nào sau đây là tốt nhất mô  tả một chữ ký  điện tử?
    1. Một phương thức chuyển giao một chữ ký viết tay vào một tài liệu điện tử
    2. Một phương pháp mã hóa thông tin bí mật
    3. Một phương pháp để cung cấp một chữ ký điện tử và mã hóa
    4. 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?
    1. 56
    2. 64
    3. 32
    4. 16
57. Các yếu tố  ảnh hưởng đến quá trình mã hóa
    1. Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền
    2. Thời gian thực hiện mã hóa và giải mã
    3. Thực hiện mã hóa khối, mở rộng số bít xử lý
    4. Tất cả đều sai
58. Đối với Firesall lọc gói, hình thức tấn công nào sau đây được thực hiện
    1. Nhái địa chỉ IP, tấn công giữa, tấn công biên
    2. Nhái địa chỉ IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ
    3. Nhái địa chỉ IP, tấn công vượt firewall,tấn công từng mẫu nhỏ
    4. 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?
    1. Adi Shamir
    2. Ross Anderson
    3. Bruce Schneier
    4. Martin Hellman
60. DES là  viết tắt của từ nào ?
    1. Data encryption system
    2. Data encryption standard
    3. Data encoding standard
    4. 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

1. Giai đoạn đầu của hacking là gì?
2. Duy trì truy cập
3. Gaining truy cập
4. Trinh sát
5. Dò tìm (Scanning)
6. Khi một hacker cố gắng tấn công một máy chủ qua Internet nó được gọi là loại tấn công?
7. Tấn công  từ xa
8. Tấn công truy cập vật lý
9. Truy cập  địa phương
10. Tấn công tấn công nội
11. Công cụ nào sau đây đúng là một công cụ để thực hiện footprinting không bị phát hiện?
    1. Whois search
    2. Traceroute
    3. Ping sweep
    4. Host scanning
12. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì?
    1. Scanning
    2. Enumeration
    3. System hacking
    4. Active information gathering
13. Footprinting là gì?
    1. đo dấu vết của một hacker có đạo đức
    2. tích luỹ dữ liệu bằng cách thu thập thông tin về một mục tiêu
    3. quét một mạng lưới mục tiêu để phát hiện hệ điều hành các loại
    4. sơ đồ bố trí vật lý của một mạng của mục tiêu
14. 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.

1. FTP sử dụng cổng gì ?

A. 21

B. 25

C. 23

D. 80

1. Cổng nào được HTTPS sử dụng?

A. 443

B. 80

C. 53

D. 21

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

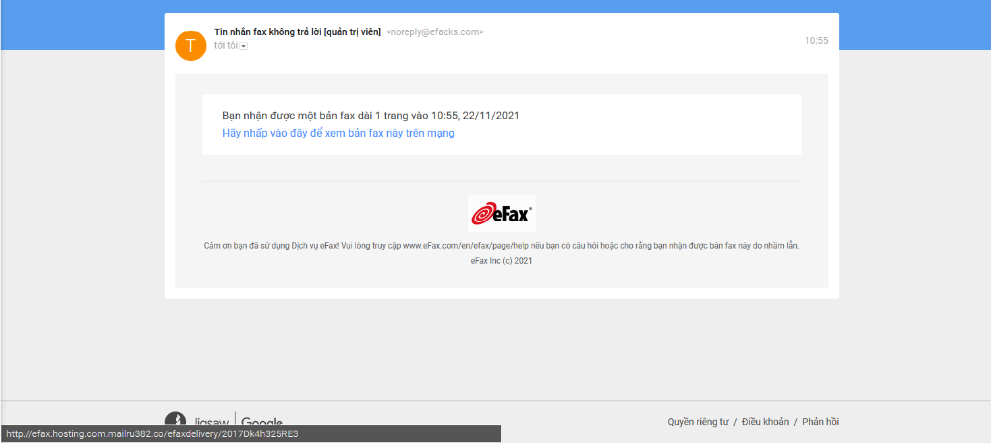
d. Thường xuyên cài đặt lại phải khi hệ thống mạng thay đổi hệ điều hành

1. Triển khai thiết bị Firewall trên môi trường kết nối mạng để làm gì? (Chọn một)
2. Kiểm soát lưu lượng mạng nào được đi, lưu lượng nào bị chặn
3. Chống người dùng cài đặt các phần mềm không an toàn lên máy tính
4. Chống trộm vào phòng máy công ty để lấy cắp dữ liệu trong ổ cứng
5. Chống dò quét sóng Wifi
6. Trên đường truyền kết nối mạng có thể mã hóa dữ liệu không? (Chọn một)
7. Có
8. Không
9. Tại sao cần đổi mật khẩu các thiết bị mạng khi sử dụng? (Chọn một)
10. Vì mật khẩu của nhà sản xuất dễ đoán và có thể tìm trên google
11. Vì mật khẩu của nhà sản xuất khó quá dễ quên
12. Vì mật khẩu của nhà sản xuất trùng với mật khẩu mạng wifi
13. Phần mềm nào sau đây là một phần mềm Anti Virus? (Chọn một)
14. Microsoft Word
15. Adobe PDF reader
16. Google Chrome
17. Kaspersky Total Security
18. Phần mềm máy tính có đặc điểm gây tác hại và có thể hoạt động ngầm được gọi là gì? (Chọn một)
19. Hệ điều hành
20. Virus (mã độc)
21. Phần mềm chat
22. Dịch vụ
23. Nhận được một email dạng “bạn ở trong danh sách những người nợ thuế, số tiền hiện tại của bạn là 50.000.000. File đính kèm là danh sách những người nợ thuế khác giống bạn. Bạn cần giúp chúng tôi chia sẻ đến tất cả những người này để họ trả đúng hạn”, theo anh/chị, đây xếp vào loại email gì? (Chọn một)
24. Phishing
25. Spam
26. Chơi khăm
27. Đâu không phải là dấu hiệu của một email tấn công phishing? (Chọn một)
28. Hình thức giống như đến từ một thương hiệu nổi tiếng hoặc cá nhân có uy tín
29. Địa chỉ email có các ký tự bất thường hoặc cố tình giả mạo các địa chỉ quen thuộc
30. Nội dung có tính chất khuyến khích click vào đường link trong email hoặc file đính kèm
31. Nội dung đưa tin quảng cáo, nhưng không chưa link hoặc file đính kèm
32. Cơ chế mã hóa nào được sử dụng trong chữ ký số? (Chọn một)
33. Mã hóa đối xứng
34. Mã hóa bất đối xứng
35. Mã hóa một phần
36. Mã hóa toàn phần
37. Cơ chế chữ ký số được sử dụng để làm gì? (Chọn một)
38. Mã hóa nội dung email
39. Xác thực người gửi và nội dung email
40. Hiển thị chữ ký gồm tên, chức danh, tên công ty của người gửi
41. Người khác không thể đọc được nội dung email
42. Làm sao để quét file đính kèm trước khi mở? (Chọn một)
43. Lưu file vào một thư mục, sau đó dùng Firewall để để scan
44. Lưu file vào một thư mục, sau đó dùng phần mềm Anti Virus để scan
45. Mở file ngay trong email thay vì lưu về máy
46. Thấy email có đính kèm là kéo thả vào thư mục Scan
47. Khi nhận email và có nghi ngờ phishing, nếu muốn kiểm tra địa chỉ người gửi có đúng hay không thì cần xem ở khu vực nào của email? (Chọn một)
48. Body
49. From (Header)
50. To
51. Signature
52. Mã độc có thể cài vào máy điện thoại thông qua phương tiện nào sau đây? (Chọn một)
53. Đính kèm email
54. App Store/Play Store
55. Trang web xấu
56. Tất cả phương án trên
57. Rủi ro “Eavesdropping” đối với điện thoại di động là gì? (Chọn một)
58. Ứng dụng app store không an toàn
59. Nghe trộm cuộc gọi
60. Cuộc gọi quảng cáo
61. Lừa đảo tống tiền
62. Số IMEI sử dụng để làm gì? (Chọn một)
63. Đăng ký SIM
64. Chính là số điện thoại để gọi
65. Bảo hành điện thoại
66. Gắn định danh duy nhất cho các thiết bị di động
67. Đâu không phải là hệ điều hành cho thiết bị di động? (Chọn một)
68. Windows mobile
69. MacOS
70. iOS
71. Android
72. Trong số liệu thống kê, các cuộc tấn công xuất hiện trên nền tảng thiết bị di động nào nhiều nhất? (Chọn một)
73. Android
74. BlackBerry
75. Windows
76. iOS
77. Chức năng mã hóa dữ liệu thẻ nhớ trên Android phone sử dụng để làm gì? (Chọn một)
78. Chống cài mã độc vào thẻ nhớ
79. Khi mất máy sẽ không bị lộ dữ liệu
80. Khi mất máy sẽ tìm lại được qua các ứng dụng của Play Store
81. Giúp tiết kiệm bộ nhớ điện thoại
82. Cách khóa SIM để kẻ xấu lấy SIM cũng không sử dụng được thế nào? (Chọn một)
83. Đặt PIN code cho SIM
84. Cài phần mềm chống tấn công SIM
85. Kết nối SIM với Internet để xác thực khi sử dụng
86. Khai báo SIM gắn với riêng IMEI điện thoại
87. Tính năng gì giúp tìm điện thoại khi mất trên iOS? (Chọn một)
88. Find our iPhone
89. iPhone finds me
90. Find my phone
91. Find my iPhone
92. Đâu không phải là một phương pháp bảo vệ thiết bị di động?
93. Cài đặt phần mềm AntiVirus, mobile security
94. Chữ ký số
95. Mã hóa bộ nhớ điện thoại
96. Cập nhật hệ điều hành
97. Đâu là 3 hình thức tấn công thiết bị di động phổ biến hiện nay?
98. Mã độc, email phishing, app phishing
99. Khai thác điểm yếu, mã độc, chiếm password
100. Mạng có dây, mạng không dây, bluetooth
101. Mã độc, khai thác điểm yếu hệ điều hành Android/iOS, Bluetooth
102. Dịch vụ đám mây công cộng (Public Cloud) khác gì với dịch vụ đám mây nội bộ (Private Cloud)? (Chọn hai)
103. Public Cloud của nhà cung cấp dịch vụ trên Internet, Private Cloud của công ty tự xây dựng, quản lý
104. Công ty chỉ cần trả tiền thuê dịch vụ sử dụng trên Public Cloud cho nhà cung cấp, còn với Private Cloud, công ty sẽ cần tự đầu tư và quản lý tất cả hạ tầng máy móc, thiết bị
105. Public cloud chỉ có ở Mỹ còn Private cloud có thể đặt ở mọi nơi
106. Public cloud tốn kém hơn do phải trả tiền thuê dịch vụ theo năm, còn Private cloud tự công ty quản lý nên không cần mất chi phí gì
107. Dịch vụ nào sau đây không thuộc loại dịch vụ đám mây (Cloud)?
108. Google Drive
109. Amazon Web Services
110. Microsoft Office 365
111. Photoshop
112. Người dùng thường bỏ qua và chấp nhận tài liệu gì khi bắt đầu sử dụng dịch vụ lưu trữ trên Cloud?
113. Cyber security law
114. Data usage law
115. Terms of service
116. Email confirmation
117. Đâu không phải là 1 trong 4 vấn đề về tính bí mật và riêng tư của dữ liệu lưu trữ trên các nhà cung cấp dịch vụ Public Cloud:
118. Mã hóa dữ liệu
119. Di chuyển dữ liệu
120. Vị trí đặt dữ liệu
121. Quyền sở hữu dữ liệu
122. Biện pháp xác thực an toàn cho phép kết hợp giữa mật khẩu với một yếu tố khác như mã OTP hoặc app xác thực trên điện thoại gọi là gì?
123. 2 way authentication
124. Data authentication
125. Multi-Factor authentication
126. Biometric authentication
127. Công ty nào sau đây có cung cấp dịch vụ hạ tầng IT (IaaS)?
128. Samsung
129. Apple
130. Toyota
131. AWS
132. Đâu không phải là hiểm họa đối với môi trường Cloud?
133. Hỏng thiết bị phần cứng
134. Phá hoại nội bộ bên trong chính nhà cung cấp cloud
135. Mất dữ liệu
136. Thất thoát dữ liệu
137. Một công ty muốn sử dụng phần mềm kế toán do một nhà cung cấp dịch vụ cung cấp qua Internet, công ty chỉ cần trả tiền theo số lượng kế toán viên sử dụng dịch vụ. Đây gọi là dịch vụ cloud gì?
138. SaaS
139. AccountingaaS
140. IaaS
141. PaaS
142. Đâu là tiêu chí lựa chọn nhà cung cấp Cloud?
143. Dịch vụ cloud an toàn đến mức nào
144. Tài nguyên tốn bao nhiêu tiền
145. Giải pháp tốt thế nào
146. Tất cả phương án trên
147. Dịch vụ cho phép công ty thuê các máy chủ ảo, có kết nối mạng để cài đặt các ứng dụng tùy chọn gọi là gì?
148. PaaS
149. CloudaaS
150. ItaaS
151. IaaS
152. Khi bạn vào quán cafe Starbucks, bạn mở máy tính và thấy một tên mạng Wifi Starbuck của quán, nhưng đồng thời cũng thấy wifi khác là Starbuck-free sóng mạnh hơn và không yêu cầu mật khẩu. Bạn có nên truy cập không và lý do là gì?
153. Không, vi đây có thể là mạng lừa đảo tấn công do lỗi cấu hình của chủ quán
154. Không, vì đây có thể là mạng lừa đảo tấn công dạng Evil Twin
155. Có, vì mạng này sóng mạnh hơn sẽ truy cập ổn định hơn
156. Có, vì mạng này miễn phí
157. Xây dựng môi trường kết nối Wireless cần có thiết bị gì?
158. Thiết bị phát sóng di động
159. Thiết bị phát sóng Wifi/Accesspoint
160. Email Server
161. Thiết bị Switch chuyển mạch
162. Trong mô hình mạng nào sau đây, những người dùng không thể kết nối trực tiếp đến nhau?
163. Internet
164. WAN
165. LAN
166. Thành phần thiết bị nào đóng vai trò kết nối cửa ngõ giữa mạng nội bộ trong gia đình với Internet?
167. Thiết bị phát sóng Wifi/Accesspoint
168. Router/Firewall
169. Máy tính cá nhân
170. Điện thoại di động
171. Bạn muốn lập một công ty với 10 người, làm việc trong cùng một văn phòng với máy tính xách tay. Bạn sẽ lựa chọn xây dựng hệ thống mạng gì cho mô hình này?
172. LAN
173. Internet
174. WAN
175. Tính năng MAC authentication khi thiết lập thiết bị Wifi accesspoint dùng để làm gì?
176. Để giới hạn truy cập đến các website xấu
177. Để thiết lập danh sách địa chỉ các máy tính/thiết bị được phép dùng mạng Wifi
178. Để quản lý các máy tính MacOS
179. Để chống mã độc MAC cho điện thoại di động
180. Thông số nào sau đây là chuẩn mã hóa bảo mật mạnh cho kết nối Wireless?
181. WEP
182. MFA
183. WPA2
184. WPA
185. Các email được lưu trữ ở đâu khi sử dụng Web mail client?
186. Trong máy tính
187. Trên server của nhà cung cấp email
188. Chỉ lưu trữ trên máy tính người nhận
189. Có các loại công cụ để sử dụng email nào (chọn hai)
190. Bưu điện
191. Giấy bút
192. Web mail client
193. Phần mềm email cài đặt trên máy tính
194. Rủi ro khi nội dung thư bị lộ lọt do gửi nhầm người trong phần To/CC là do đâu
195. Giả mạo
196. Lỗi người dùng
197. Hacker
198. Email server
199. Hệ thống tiếp nhận, chuyển tiếp bức thư giữa người gửi với người nhận gọi là gì
200. Service provider
201. Web server
202. Email client
203. Email server
204. Người dùng khi soạn thảo email và gửi đến người nhận, bức thư sẽ đi thẳng đến máy tính người nhận mà không qua bất kỳ trung gian nào, đúng hay sai?
205. Đúng
206. Sai
207. Công ty bạn muốn thanh lý lô máy tính hết khấu hao sử dụng. Các máy tính này lưu nhiều dữ liệu về hoạt động của công ty, đội IT cần làm gì để đảm bảo dữ liệu không bị lộ lọt ra bên ngoài khi bán thanh lý máy tính và vẫn bán được nguyên máy?
208. Vào hệ điều hành, chọn các thư mục chứa dữ liệu và bấm nút Shift + Delete để xóa vĩnh viễn hết dữ liệu trên ổ cứng trước khi bán
209. Sử dụng phần mềm để “wipe” ổ cứng, phần mềm sẽ xóa và chèn nội dung ngẫu nhiên vào toàn bộ ổ cứng để không khôi phục được dữ liệu
210. Tháo riêng ổ cứng và phá hủy cơ học
211. Tính năng sao lưu có sẵn trên hệ điều hành MacOS gọi là gì?
212. Disk machine
213. Time Machine
214. Time recover
215. File History
216. Tính năng sao lưu dữ liệu trên hệ điều hành Windows gọi là gì?
217. Data store
218. Data history
219. File history
220. Full store
221. Đâu không phải là dịch vụ sao lưu dữ liệu online?
222. Play Store
223. iCloud
224. Microsoft OneDrive
225. Google Drive
226. Hình thức sao lưu dữ liệu nào chỉ ghi lại những thay đổi so với lần sao lưu Full gần nhất?
227. Full+
228. Partial
229. Differential
230. Incremental
231. Trong số liệu báo cáo về tấn công email, số lượng lớn nhất thuộc về loại tấn công gì?
232. Malware
233. Phishing
234. BEC
235. Hình thức sao lưu dữ liệu nào cần nhiều bộ nhớ nhất nhưng thời gian khôi phục lại là nhanh nhất?
236. Incremental
237. Differential
238. Full
239. Partial
240. Có mấy hình thức sao lưu dữ liệu?
241. 2
242. 3
243. 4
244. 5
245. Thảm họa thiên nhiên có phải là rủi ro làm mất dữ liệu không?
246. Có
247. Không
248. Sao lưu dữ liệu giúp hạn chế được những rủi ro gì? (Chọn hai)
249. Lấy cắp dữ liệu
250. Lộ lọt dữ liệu ra ngoài
251. Hỏng hệ thống phần cứng lưu trữ dữ liệu
252. Lỗi người dùng làm hỏng dữ liệu
253. Sao lưu dữ liệu là làm gì?
254. Nhân bản dữ liệu và lưu trữ cùng bản gốc trên cùng máy tính/điện thoại
255. Copy dữ liệu sang một hệ thống khác để khôi phục lại khi cần
256. In tài liệu ra thành bản cứng
257. Đặt mật khẩu cho dữ liệu để người khác không đọc được
258. Tính năng nào của Facebook cho phép người dùng kiểm tra và tùy biến các thiết lập về riêng tư?
259. Security and Login
260. Privacy Checkup
261. Public blocking
262. Timeline
263. Những trang nào sau đây không phải của mạng xã hội facebook (chọn hai)?
264. help-facebook.facebob.com
265. data.faceb00k.com
266. [www.facebook.com](http://www.facebook.com)
267. [www.facabook.com](http://www.facabook.com)
268. Tính năng nào nên tắt khi chụp ảnh, đăng bài từ điện thoại để tránh bị kẻ xấu theo dõi vị trí, thói quen?
269. Geo Tagging/Location
270. Google map
271. Apple map
272. GPS
273. Kỹ thuật nào của hacker tiếp xúc trực tiếp với đối tượng tấn công thông qua mạng xã hội, nói chuyện, chat?
274. Malware
275. Command and control
276. Social engineering
277. Phishing
278. Tính năng nào có thể giúp hacker lấy được mật khẩu dựa trên thông tin được cung cấp trên facebook profile?
279. Forgot password
280. Hỏi mật khẩu thông qua người thân
281. Đường link lừa đảo trong email phishing
282. Nghe trộm
283. Cách nhận biết các trang web giả dạng, lừa đảo trên mạng xã hội là gì?
284. Xem kỹ URL của trang web trên thanh địa chỉ của trình duyệt xem có phải đến từ facebook.com hay các trang mạng xã hội tương tự hay không
285. Gọi điện hỏi hỗ trợ kỹ thuật của nhà cung cấp mạng xã hội
286. Bật tính năng firewall trên hệ điều hành
287. Báo IT của công ty hỗ trợ
288. Hình thức lừa đảo bằng việc gửi email giả mạo giống hình thức của facebook để lừa lấy mật khẩu của người dùng gọi là gì?
289. Spam mail
290. Hacking
291. Phishing
292. Mã độc
293. Khi nhận được email có phần From là tên của CEO của công ty và chứa file đính kèm, với nội dung yêu cầu mở file đính kèm để làm một việc gì đó, bạn cần làm gì để đảm bảo an toàn cho máy tính của mình?
294. Bấm vào phần From để kiểm tra địa chỉ email đầy đủ có đúng là của CEO không
295. Không mở những email như vậy
296. Mở file và xử lý ngay công việc do đây là email từ CEO
297. Trường thông tin nào trong profile mạng xã hội facebook được khuyến nghị nên ẩn đi không cho người khác đọc được?
298. Giới tính
299. Ngày sinh
300. Ảnh đại diện
301. Tên
302. Thông tin gì sau đây không nên công khai trên mạng xã hội (chọn ba)
303. Địa chỉ email công việc
304. Địa chỉ email cá nhân
305. Địa chỉ nơi làm việc
306. Số CMND
307. Khi sử dụng Facebook messenger, khi có bất cứ ai gửi cho bạn một file văn bản .doc, biện pháp nào là phù hợp nhất để đảm bảo an toàn cho máy tính của mình?
308. Mở ngay file ra đọc
309. Tải file về nhưng chưa mở ngay mà quét virus bằng phần mềm Anti Virus trước, nếu an toàn thì mới mở
310. Gửi file cho bộ phận IT của công ty để phân tích mã độc, nếu an toàn thì mới mở
311. Tải file về, đổi tên file thành “safe” sau đó mở file để đọc
312. Chức năng nào của Zalo cho phép không tự động tải về máy tính các file người khác gửi qua chat
313. Quét file trước khi tải
314. Tắt tự động tải trước
315. Tự động tải file
316. Tự động tải sau
317. Đâu không phải là vấn đề an ninh trong môi trường chat?
318. Chiếm quyền máy chủ
319. Lỗ hổng phần mềm
320. Mã độc
321. Lừa đảo
322. Mục nào sau đây sử dụng để thiết lập các tính năng an toàn cho trình duyệt Chrome:
323. Browser > Health > Security
324. Setting > Privacy and Security
325. Configuration > Safety and data privacy
326. Configuration > Security
327. Tính năng nào của trình duyệt cho phép lưu lại những đoạn thông tin như đăng nhập, giỏ hàng và các tùy chọn khác để khi truy cập web thì người dùng không cần khai báo lại?
328. Java script
329. Plugin
330. URL
331. Cookie
332. Đâu không phải tên của một trình duyệt
333. Android
334. Chrome
335. Safari
336. Firefox
337. Các thông tin nào sau đây được coi là thông tin cá nhân (PII - Personally Identifiable Information) cần được bảo vệ
338. Số hộ chiếu/ số thẻ căn cước công dân
339. Số thẻ tín dụng
340. Mã số thuế cá nhân
341. Tất cả thông tin trên
342. Triển khai thiết bị Firewall trên môi trường kết nối mạng để làm gì?
343. Kiểm soát lưu lượng mạng nào được đi, lưu lượng nào bị chặn
344. Chống người dùng cài đặt các phần mềm không an toàn lên máy tính
345. Chống trộm vào phòng máy công ty để lấy cắp dữ liệu trong ổ cứng
346. Chống dò quét sóng Wifi
347. Trên đường truyền kết nối mạng có thể mã hóa dữ liệu không?
348. Có
349. Không
350. Tại sao cần đổi mật khẩu các thiết bị mạng khi sử dụng
351. Vì mật khẩu của nhà sản xuất dễ đoán và có thể tìm trên google
352. Vì mật khẩu của nhà sản xuất khó quá dễ quên
353. Vì mật khẩu của nhà sản xuất trùng với mật khẩu mạng wifi
354. Khi truy cập web ở mạng wifi công cộng như quán cafe thì nên làm gì để kết nối an toàn?
355. Sử dụng chương trình VPN
356. Sử dụng điện thoại thay vì máy tính
357. Chỉ sử dụng Chrome, không dùng Safari hay Firefox
358. Truy cập web thông qua chương trình email
359. Đâu không phải là mối nguy hại trên Internet?
360. Mất trộm máy tính
361. Lấy cắp dữ liệu
362. Lấy cắp định danh
363. Sự riêng tư và bí mật dữ liệu trao đổi
364. Chương trình trên máy tính, sử dụng giao thức HTTP để truy cập đến các trang web được gọi là gì?
365. Skype
366. Windows Explorer
367. Trình duyệt
368. Phần mềm Email
369. Cơ chế phần mềm diệt Virus quét toàn bộ máy tính để kiểm tra xem có mã độc không gọi là gì?
370. Scan
371. Signature
372. Compare
373. Quarantine
374. Bộ cơ sở dữ liệu của phần mềm diệt Virus (Anti Virus) để phát hiện mã độc bằng cách so sánh mã độc với bộ nhận diện có sẵn gọi là gì?
375. Behavior
376. Scan
377. Signature
378. Kaspersky
379. Đâu không phải là một hành động của phần mềm Anti Virus?
380. Alert
381. Quarantine
382. Clean
383. Clone
384. Làm thế nào để hacker từ ngoài Internet có thể điều khiển hoạt động trên máy tính của nạn nhân?
385. Hacker không thể điều khiển được
386. Mã độc làm tất cả mọi việc thay cho hacker
387. Mã độc tạo kênh điều khiển qua Internet đến máy tính của Hacker
388. Đâu không phải là triệu chứng máy tính nhiễm mã độc
389. Qua thời gian, ổ cứng dần đầy lên
390. Các chức năng bảo mật của hệ điều hành tự nhiên bị tắt
391. Chậm, CPU và RAM % cao
392. Màn hình xanh (Crash)
393. Ransomware có chức năng chính là gì?
394. Mã hóa dữ liệu máy tính và tống tiền
395. Tạo các cửa hậu để hacker xâm nhập điều khiển máy tính
396. Dò quét mật khẩu của người quản trị trên hệ điều hành
397. Lấy cắp thông tin của tổ chức và gửi ra ngoài
398. Chức năng nào sau đây không phải của Trojan
399. Giả dạng các phần mềm hợp lệ như game, nghe nhạc, tiện ích
400. Xâm nhập qua việc đính kèm vào ảnh, video, file văn bản…
401. Mã hóa toàn bộ dữ liệu máy tính và tống tiền
402. Đặc điểm của Worm khác biệt so với các loại mã độc khác là gì?
403. Có khả năng ẩn danh trong hệ điều hành
404. Có khả năng tự lây lan trong mạng
405. Có khả năng tự hủy
406. Có khả năng tự thay đổi
407. Trojan có phải một loại mã độc không?
408. Có
409. Không
410. Hacker từ ngoài Internet có thể khiến máy tính của người dùng bị mã độc thông qua cách nào sau đây?
411. Cắm USB có chứa mã độc vào máy tính của nạn nhân
412. Gửi email có nội dung lừa đảo để người dùng click vào file đính kèm chưa mã độc
413. Gửi file chưa mã độc từ máy tính hacker đến máy tính nạn nhân trực tiếp
414. Hacker không thể nào làm máy tính của người dùng nhiễm mã độc
415. Việc đặt mật khẩu cho file văn bản trước khi gửi cho người khác là để đảm bảo thuộc tính nào của dữ liệu?
416. Tính sẵn sàng
417. Tính bí mật
418. Tính xác thực
419. Tính công khai
420. Tại sao cần có bước After khi triển khai an ninh dữ liệu?
421. Vì After là để duy trì trạng thái an ninh an toàn của hệ thống
422. Vì After là để thiết lập các biện pháp phòng thủ, phòng chống cho hệ thống
423. Vì con người hay bỏ qua bước Before và During
424. Vì các giải pháp phòng chống tấn công đôi khi không đủ an toàn 100%
425. Cài đặt phần mềm diệt Virus thuộc bước nào trong 3 bước triển khai an ninh dữ liệu?
426. Never
427. After
428. During
429. Before
430. Đâu không phải là một tổn thất khi mất an ninh dữ liệu?
431. Mất tính sẵn sàng
432. Tổn thất lòng tin
433. Tổn thất tài chính
434. Tổn thất tinh thần
435. Phương thức nào sau đây thuộc biện pháp an ninh dữ liệu vật lý (Physical)?
436. Khóa vân tay cho phòng làm việc﻿
437. Bảo vệ truy cập mạng Wifi công ty
438. Nội quy, quy định sử dụng máy tính an toàn
439. Cài đặt phần mềm diệt virus
440. Ba hiểm họa đối với dữ liệu trong bài bao gồm:
441. Thảm họa tự nhiên, người sử dụng, hiểm họa từ kẻ tấn công bên ngoài
442. Người sử dụng, người quản lý, người bên ngoài
443. Người bên trong tổ chức, đối thủ cạnh tranh, hacker tự do
444. Cái gì sau đây không phải là dữ liệu hữu hình?
445. File văn bản doc trên máy tính
446. Ảnh chụp gia đình
447. Hồ sơ dự thầu của công ty
448. Danh tiếng của công ty
449. Data Breach là gì?
450. Hỏng dữ liệu
451. Mất dữ liệu
452. Thất thoát dữ liệu
453. Thay đổi dữ liệu
454. Khi cần kiểm soát các kết nối mạng vào/ra máy tính cá nhân, bạn sẽ dùng chức năng nào trên Windows và Mac?
455. Anti Virus
456. Firewall
457. Google Chrome
458. Encryption
459. Tính năng EFS và Bitlocker trên Windows khác gì nhau?
460. EFS để mã hóa toàn bộ ổ cứng máy tính, còn Bitlocker dùng để mã hóa từng file/folder
461. EFS để mã hóa từng file/folder, còn Bitlocker dùng để mã hóa toàn bộ ổ cứng
462. EFS dùng để mã hóa còn Bitlocker dùng để chống mã độc
463. Bitlocker dùng để mã hóa còn EFS dùng để chống mã độc
464. Mật khẩu máy tính nào sau đây đủ mạnh?
465. Password
466. 66668888
467. M@tkha
468. Maytinhcuatoiratantoan
469. Nếu bạn có một thư mục chứa nội dung quan trọng và máy tính sử dụng chung cùng người khác, bạn nên làm gì để người khác không nhìn được thư mục này trên máy?
470. Mã hóa toàn bộ ổ cứng
471. Nâng mức cảnh báo an ninh cho hệ điều hành
472. Dùng chức năng Windows Firewall để chặn người khác không truy cập được file
473. Dùng chức năng ẩn file và folder
474. Chức năng mã hóa ổ cứng trên máy tính MacOS gọi là gì?
475. BitLocker
476. File encryptor
477. FileVault
478. MacVault
479. Vì sao cần khóa máy tính khi không sử dụng?
480. Để tiết kiệm điện
481. Để máy tính bền hơn
482. Để tránh người khác truy cập máy tính khi chúng ta không có mặt
483. Để chống mã độc xâm nhập từ Internet
484. Tính năng nào giúp hệ điều hành Windows cập nhật sửa lỗi phần mềm và các lỗ hổng bảo mật?
485. Windows Firewall
486. Windows Defender
487. Windows Update
488. indows Explorer
489. Tính năng nào của Windows giúp chống các Virus và Threat trên máy tính?
490. Windows Defender
491. Windows Firewall
492. Windows Malware
493. Windows Bitlocker
494. Tại sao cần mã hóa ổ cứng máy tính xách tay?
495. Để ngắt truy cập Internet của máy
496. Để nếu mất máy sẽ không bị lộ dữ liệu cho người khác
497. Để tránh bị mã độc tống tiền tấn công
498. Để bảo vệ dữ liệu không bị hỏng hóc
499. Hệ điều hành là gì?
500. Là hệ thống các linh kiện phần cứng máy tính như CPU, RAM, ổ cứng
501. Là phần mềm điều khiển trung gian, tiếp nhận lệnh từ người dùng và quản lý các phần cứng máy tính
502. Là phần mềm cài đặt trên Windows hoặc MacOS
503. Là tổ chức của Hacker cho phép điều khiển các cuộc tấn công
504. Trên đường truyền kết nối mạng có thể mã hóa dữ liệu không? (Chọn một)
505. Có
506. Không
507. Tại sao cần đổi mật khẩu các thiết bị mạng khi sử dụng? (Chọn một)
508. Vì mật khẩu của nhà sản xuất dễ đoán và có thể tìm trên google
509. Vì mật khẩu của nhà sản xuất khó quá dễ quên
510. Vì mật khẩu của nhà sản xuất trùng với mật khẩu mạng wifi
511. Phần mềm nào sau đây là một phần mềm Anti Virus? (Chọn một)
512. Microsoft Word
513. Adobe PDF reader
514. Google Chrome
515. Kaspersky Total Security
516. Phần mềm máy tính có đặc điểm gây tác hại và có thể hoạt động ngầm được gọi là gì? (Chọn một)
517. Hệ điều hành
518. Virus (mã độc)
519. Phần mềm chat
520. Dịch vụ
521. Đâu không phải là dấu hiệu của một email tấn công phishing? (Chọn một)
522. Hình thức giống như đến từ một thương hiệu nổi tiếng hoặc cá nhân có uy tín
523. Địa chỉ email có các ký tự bất thường hoặc cố tình giả mạo các địa chỉ quen thuộc
524. Nội dung có tính chất khuyến khích click vào đường link trong email hoặc file đính kèm
525. Nội dung đưa tin quảng cáo, nhưng không chưa link hoặc file đính kèm
526. Cơ chế chữ ký số được sử dụng để làm gì? (Chọn một)
527. Mã hóa nội dung email
528. Xác thực người gửi và nội dung email
529. Hiển thị chữ ký gồm tên, chức danh, tên công ty của người gửi
530. Người khác không thể đọc được nội dung email
531. Làm sao để quét file đính kèm trước khi mở? (Chọn một)
532. Lưu file vào một thư mục, sau đó dùng Firewall để để scan
533. Lưu file vào một thư mục, sau đó dùng phần mềm Anti Virus để scan
534. Mở file ngay trong email thay vì lưu về máy
535. Thấy email có đính kèm là kéo thả vào thư mục Scan
536. Khi nhận email và có nghi ngờ phishing, nếu muốn kiểm tra địa chỉ người gửi có đúng hay không thì cần xem ở khu vực nào của email? (Chọn một)
537. Body
538. From (Header)
539. To
540. Signature
541. Mã độc có thể cài vào máy điện thoại thông qua phương tiện nào sau đây? (Chọn một)
542. Triển khai 02 cấp tỉnh – huyện, phục vụ hoạt động nhiều cơ quan, tổ chứcĐính kèm email
543. App Store/Play Store
544. Trang web xấu
545. Tất cả phương án trên
546. Rủi ro “Eavesdropping” đối với điện thoại di động là gì? (Chọn một)
547. Ứng dụng app store không an toàn
548. Nghe trộm cuộc gọi
549. Cuộc gọi quảng cáo
550. Lừa đảo tống tiền
551. Số IMEI sử dụng để làm gì? (Chọn một)
552. Đăng ký SIM
553. Chính là số điện thoại để gọi
554. Bảo hành điện thoại
555. Gắn định danh duy nhất cho các thiết bị di động
556. Cách khóa SIM để kẻ xấu lấy SIM cũng không sử dụng được thế nào? (Chọn một)
557. Đặt PIN code cho SIM
558. Cài phần mềm chống tấn công SIM
559. Kết nối SIM với Internet để xác thực khi sử dụng
560. Khai báo SIM gắn với riêng IMEI điện thoại
561. Tính năng gì giúp tìm điện thoại khi mất trên iOS? (Chọn một)
562. Find our iPhone
563. iPhone finds me
564. Find my phone
565. Find my iPhone
566. Đâu không phải là một phương pháp bảo vệ thiết bị di động?
567. Cài đặt phần mềm AntiVirus, mobile security
568. Chữ ký số
569. Mã hóa bộ nhớ điện thoại
570. Cập nhật hệ điều hành
571. Đâu là 3 hình thức tấn công thiết bị di động phổ biến hiện nay?
572. Mã độc, email phishing, app phishing
573. Khai thác điểm yếu, mã độc, chiếm password
574. Mạng có dây, mạng không dây, bluetooth
575. Mã độc, khai thác điểm yếu hệ điều hành Android/iOS, Bluetooth
576. Biện pháp xác thực an toàn cho phép kết hợp giữa mật khẩu với một yếu tố khác như mã OTP hoặc app xác thực trên điện thoại gọi là gì?
577. 2 way authentication
578. Data authentication
579. Multi-Factor authentication
580. Biometric authentication
581. Công ty nào sau đây có cung cấp dịch vụ hạ tầng IT (IaaS)?
582. Samsung
583. Apple
584. Toyota
585. AWS
586. Đâu không phải là hiểm họa đối với môi trường Cloud?
587. Hỏng thiết bị phần cứng
588. Phá hoại nội bộ bên trong chính nhà cung cấp cloud
589. Mất dữ liệu
590. Thất thoát dữ liệu
591. Một công ty muốn sử dụng phần mềm kế toán do một nhà cung cấp dịch vụ cung cấp qua Internet, công ty chỉ cần trả tiền theo số lượng kế toán viên sử dụng dịch vụ. Đây gọi là dịch vụ cloud gì?
592. SaaS
593. AccountingaaS
594. IaaS
595. PaaS
596. Đâu là tiêu chí lựa chọn nhà cung cấp Cloud?
597. Dịch vụ cloud an toàn đến mức nào
598. Tài nguyên tốn bao nhiêu tiền
599. Giải pháp tốt thế nào
600. Tất cả phương án trên
601. Dịch vụ cho phép công ty thuê các máy chủ ảo, có kết nối mạng để cài đặt các ứng dụng tùy chọn gọi là gì?
602. PaaS
603. CloudaaS
604. ItaaS
605. IaaS
606. Khi bạn vào quán cafe Starbucks, bạn mở máy tính và thấy một tên mạng Wifi Starbuck của quán, nhưng đồng thời cũng thấy wifi khác là Starbuck-free sóng mạnh hơn và không yêu cầu mật khẩu. Bạn có nên truy cập không và lý do là gì?
607. Không, vi đây có thể là mạng lừa đảo tấn công do lỗi cấu hình của chủ quán
608. Không, vì đây có thể là mạng lừa đảo tấn công dạng Evil Twin
609. Có, vì mạng này sóng mạnh hơn sẽ truy cập ổn định hơn
610. Có, vì mạng này miễn phí
611. Xây dựng môi trường kết nối Wireless cần có thiết bị gì?
612. Thiết bị phát sóng di động
613. Thiết bị phát sóng Wifi/Accesspoint
614. Email Server
615. Thiết bị Switch chuyển mạch
616. Trong mô hình mạng nào sau đây, những người dùng không thể kết nối trực tiếp đến nhau?
617. Internet
618. WAN
619. LAN
620. Thành phần thiết bị nào đóng vai trò kết nối cửa ngõ giữa mạng nội bộ trong gia đình với Internet?
621. Thiết bị phát sóng Wifi/Accesspoint
622. Router/Firewall
623. Máy tính cá nhân
624. Điện thoại di động
625. Bạn muốn lập một công ty với 10 người, làm việc trong cùng một văn phòng với máy tính xách tay. Bạn sẽ lựa chọn xây dựng hệ thống mạng gì cho mô hình này?
626. LAN
627. Internet
628. WAN
629. Tính năng MAC authentication khi thiết lập thiết bị Wifi accesspoint dùng để làm gì?
630. Để giới hạn truy cập đến các website xấu
631. Để thiết lập danh sách địa chỉ các máy tính/thiết bị được phép dùng mạng Wifi
632. Để quản lý các máy tính MacOS
633. Để chống mã độc MAC cho điện thoại di động
634. Thông số nào sau đây là chuẩn mã hóa bảo mật mạnh cho kết nối Wireless?
635. WEP
636. MFA
637. WPA2
638. WPA
639. Các email được lưu trữ ở đâu khi sử dụng Web mail client?
640. Trong máy tính
641. Trên server của nhà cung cấp email
642. Chỉ lưu trữ trên máy tính người nhận
643. Có các loại công cụ để sử dụng email nào (chọn hai)
644. Bưu điện
645. Giấy bút
646. Web mail client
647. Phần mềm email cài đặt trên máy tính
648. Rủi ro khi nội dung thư bị lộ lọt do gửi nhầm người trong phần To/CC là do đâu
649. Giả mạo
650. Lỗi người dùng
651. Hacker
652. Email server
653. Hệ thống tiếp nhận, chuyển tiếp bức thư giữa người gửi với người nhận gọi là gì
654. Service provider
655. Web server
656. Email client
657. Email server
658. Người dùng khi soạn thảo email và gửi đến người nhận, bức thư sẽ đi thẳng đến máy tính người nhận mà không qua bất kỳ trung gian nào, đúng hay sai?
659. Đúng
660. Sai
661. Công ty bạn muốn thanh lý lô máy tính hết khấu hao sử dụng. Các máy tính này lưu nhiều dữ liệu về hoạt động của công ty, đội IT cần làm gì để đảm bảo dữ liệu không bị lộ lọt ra bên ngoài khi bán thanh lý máy tính và vẫn bán được nguyên máy?
662. Vào hệ điều hành, chọn các thư mục chứa dữ liệu và bấm nút Shift + Delete để xóa vĩnh viễn hết dữ liệu trên ổ cứng trước khi bán
663. Sử dụng phần mềm để “wipe” ổ cứng, phần mềm sẽ xóa và chèn nội dung ngẫu nhiên vào toàn bộ ổ cứng để không khôi phục được dữ liệu
664. Tháo riêng ổ cứng và phá hủy cơ học
665. Tính năng sao lưu có sẵn trên hệ điều hành MacOS gọi là gì?
666. Disk machine
667. Time Machine
668. Time recover
669. File History
670. Tính năng sao lưu dữ liệu trên hệ điều hành Windows gọi là gì?
671. Data store
672. Data history
673. File history
674. Full store
675. Đâu không phải là dịch vụ sao lưu dữ liệu online?
676. Play Store
677. iCloud
678. Microsoft OneDrive
679. Google Drive
680. Hình thức sao lưu dữ liệu nào chỉ ghi lại những thay đổi so với lần sao lưu Full gần nhất?
681. Full+
682. Partial
683. Differential
684. Incremental
685. Trong số liệu báo cáo về tấn công email, số lượng lớn nhất thuộc về loại tấn công gì?
686. Malware
687. Phishing
688. BEC
689. Hình thức sao lưu dữ liệu nào cần nhiều bộ nhớ nhất nhưng thời gian khôi phục lại là nhanh nhất?
690. Incremental
691. Differential
692. Full
693. Partial
694. Có mấy hình thức sao lưu dữ liệu?
695. 2
696. 3
697. 4
698. 5
699. Thảm họa thiên nhiên có phải là rủi ro làm mất dữ liệu không?
700. Có
701. Không
702. Sao lưu dữ liệu giúp hạn chế được những rủi ro gì? (Chọn hai)
703. Lấy cắp dữ liệu
704. Lộ lọt dữ liệu ra ngoài
705. Hỏng hệ thống phần cứng lưu trữ dữ liệu
706. Lỗi người dùng làm hỏng dữ liệu
707. Sao lưu dữ liệu là làm gì?
708. Nhân bản dữ liệu và lưu trữ cùng bản gốc trên cùng máy tính/điện thoại
709. Copy dữ liệu sang một hệ thống khác để khôi phục lại khi cần
710. In tài liệu ra thành bản cứng
711. Đặt mật khẩu cho dữ liệu để người khác không đọc được
712. Tính năng nào của Facebook cho phép người dùng kiểm tra và tùy biến các thiết lập về riêng tư?
713. Security and Login
714. Privacy Checkup
715. Public blocking
716. Timeline
717. Những trang nào sau đây không phải của mạng xã hội facebook (chọn hai)?
718. help-facebook.facebob.com
719. data.faceb00k.com
720. [www.facebook.com](http://www.facebook.com)
721. [www.facabook.com](http://www.facabook.com)
722. Tính năng nào nên tắt khi chụp ảnh, đăng bài từ điện thoại để tránh bị kẻ xấu theo dõi vị trí, thói quen?
723. Geo Tagging/Location
724. Google map
725. Apple map
726. GPS
727. Kỹ thuật nào của hacker tiếp xúc trực tiếp với đối tượng tấn công thông qua mạng xã hội, nói chuyện, chat?
728. Malware
729. Command and control
730. Social engineering
731. Phishing
732. Tính năng nào có thể giúp hacker lấy được mật khẩu dựa trên thông tin được cung cấp trên facebook profile?
733. Forgot password
734. Hỏi mật khẩu thông qua người thân
735. Đường link lừa đảo trong email phishing
736. Nghe trộm
737. Cách nhận biết các trang web giả dạng, lừa đảo trên mạng xã hội là gì?
738. Xem kỹ URL của trang web trên thanh địa chỉ của trình duyệt xem có phải đến từ facebook.com hay các trang mạng xã hội tương tự hay không
739. Gọi điện hỏi hỗ trợ kỹ thuật của nhà cung cấp mạng xã hội
740. Bật tính năng firewall trên hệ điều hành
741. Báo IT của công ty hỗ trợ
742. Hình thức lừa đảo bằng việc gửi email giả mạo giống hình thức của facebook để lừa lấy mật khẩu của người dùng gọi là gì?
743. Spam mail
744. Hacking
745. Phishing
746. Mã độc
747. Khi nhận được email có phần From là tên của CEO của công ty và chứa file đính kèm, với nội dung yêu cầu mở file đính kèm để làm một việc gì đó, bạn cần làm gì để đảm bảo an toàn cho máy tính của mình?
748. Bấm vào phần From để kiểm tra địa chỉ email đầy đủ có đúng là của CEO không
749. Không mở những email như vậy
750. Mở file và xử lý ngay công việc do đây là email từ CEO
751. Trường thông tin nào trong profile mạng xã hội facebook được khuyến nghị nên ẩn đi không cho người khác đọc được?
752. Giới tính
753. Ngày sinh
754. Ảnh đại diện
755. Tên
756. Thông tin gì sau đây không nên công khai trên mạng xã hội (chọn ba)
757. Địa chỉ email công việc
758. Địa chỉ email cá nhân
759. Địa chỉ nơi làm việc
760. Số CMND
761. Khi sử dụng Facebook messenger, khi có bất cứ ai gửi cho bạn một file văn bản .doc, biện pháp nào là phù hợp nhất để đảm bảo an toàn cho máy tính của mình?
762. Mở ngay file ra đọc
763. Tải file về nhưng chưa mở ngay mà quét virus bằng phần mềm Anti Virus trước, nếu an toàn thì mới mở
764. Gửi file cho bộ phận IT của công ty để phân tích mã độc, nếu an toàn thì mới mở
765. Tải file về, đổi tên file thành “safe” sau đó mở file để đọc
766. Chức năng nào của Zalo cho phép không tự động tải về máy tính các file người khác gửi qua chat
767. Quét file trước khi tải
768. Tắt tự động tải trước
769. Tự động tải file
770. Tự động tải sau
771. Đâu không phải là vấn đề an ninh trong môi trường chat?
772. Chiếm quyền máy chủ
773. Lỗ hổng phần mềm
774. Mã độc
775. Lừa đảo
776. Mục nào sau đây sử dụng để thiết lập các tính năng an toàn cho trình duyệt Chrome:
777. Browser > Health > Security
778. Setting > Privacy and Security
779. Configuration > Safety and data privacy
780. Configuration > Security
781. Tính năng nào của trình duyệt cho phép lưu lại những đoạn thông tin như đăng nhập, giỏ hàng và các tùy chọn khác để khi truy cập web thì người dùng không cần khai báo lại?
782. Java script
783. Plugin
784. URL
785. Cookie
786. Đâu không phải tên của một trình duyệt
787. Android
788. Chrome
789. Safari
790. Firefox
791. Các thông tin nào sau đây được coi là thông tin cá nhân (PII - Personally Identifiable Information) cần được bảo vệ
792. Số hộ chiếu/ số thẻ căn cước công dân
793. Số thẻ tín dụng
794. Mã số thuế cá nhân
795. Tất cả thông tin trên
796. Triển khai thiết bị Firewall trên môi trường kết nối mạng để làm gì?
797. Kiểm soát lưu lượng mạng nào được đi, lưu lượng nào bị chặn
798. Chống người dùng cài đặt các phần mềm không an toàn lên máy tính
799. Chống trộm vào phòng máy công ty để lấy cắp dữ liệu trong ổ cứng
800. Chống dò quét sóng Wifi
801. Trên đường truyền kết nối mạng có thể mã hóa dữ liệu không?
802. Có
803. Không
804. Tại sao cần đổi mật khẩu các thiết bị mạng khi sử dụng
805. Vì mật khẩu của nhà sản xuất dễ đoán và có thể tìm trên google
806. Vì mật khẩu của nhà sản xuất khó quá dễ quên
807. Vì mật khẩu của nhà sản xuất trùng với mật khẩu mạng wifi
808. Khi truy cập web ở mạng wifi công cộng như quán cafe thì nên làm gì để kết nối an toàn?
809. Sử dụng chương trình VPN
810. Sử dụng điện thoại thay vì máy tính
811. Chỉ sử dụng Chrome, không dùng Safari hay Firefox
812. Truy cập web thông qua chương trình email
813. Đâu không phải là mối nguy hại trên Internet?
814. Mất trộm máy tính
815. Lấy cắp dữ liệu
816. Lấy cắp định danh
817. Sự riêng tư và bí mật dữ liệu trao đổi
818. Chương trình trên máy tính, sử dụng giao thức HTTP để truy cập đến các trang web được gọi là gì?
819. Skype
820. Windows Explorer
821. Trình duyệt
822. Phần mềm Email
823. Cơ chế phần mềm diệt Virus quét toàn bộ máy tính để kiểm tra xem có mã độc không gọi là gì?
824. Scan
825. Signature
826. Compare
827. Quarantine
828. Bộ cơ sở dữ liệu của phần mềm diệt Virus (Anti Virus) để phát hiện mã độc bằng cách so sánh mã độc với bộ nhận diện có sẵn gọi là gì?
829. Behavior
830. Scan
831. Signature
832. Kaspersky
833. Đâu không phải là một hành động của phần mềm Anti Virus?
834. Alert
835. Quarantine
836. Clean
837. Clone
838. Làm thế nào để hacker từ ngoài Internet có thể điều khiển hoạt động trên máy tính của nạn nhân?
839. Hacker không thể điều khiển được
840. Mã độc làm tất cả mọi việc thay cho hacker
841. Mã độc tạo kênh điều khiển qua Internet đến máy tính của Hacker
842. Đâu không phải là triệu chứng máy tính nhiễm mã độc
843. Qua thời gian, ổ cứng dần đầy lên
844. Các chức năng bảo mật của hệ điều hành tự nhiên bị tắt
845. Chậm, CPU và RAM % cao
846. Màn hình xanh (Crash)
847. Ransomware có chức năng chính là gì?
848. Mã hóa dữ liệu máy tính và tống tiền
849. Tạo các cửa hậu để hacker xâm nhập điều khiển máy tính
850. Dò quét mật khẩu của người quản trị trên hệ điều hành
851. Lấy cắp thông tin của tổ chức và gửi ra ngoài
852. Chức năng nào sau đây không phải của Trojan
853. Giả dạng các phần mềm hợp lệ như game, nghe nhạc, tiện ích
854. Xâm nhập qua việc đính kèm vào ảnh, video, file văn bản…
855. Mã hóa toàn bộ dữ liệu máy tính và tống tiền
856. Đặc điểm của Worm khác biệt so với các loại mã độc khác là gì?
857. Có khả năng ẩn danh trong hệ điều hành
858. Có khả năng tự lây lan trong mạng
859. Có khả năng tự hủy
860. Có khả năng tự thay đổi
861. Trojan có phải một loại mã độc không?
862. Có
863. Không
864. Hacker từ ngoài Internet có thể khiến máy tính của người dùng bị mã độc thông qua cách nào sau đây?
865. Cắm USB có chứa mã độc vào máy tính của nạn nhân
866. Gửi email có nội dung lừa đảo để người dùng click vào file đính kèm chưa mã độc
867. Gửi file chưa mã độc từ máy tính hacker đến máy tính nạn nhân trực tiếp
868. Hacker không thể nào làm máy tính của người dùng nhiễm mã độc
869. Việc đặt mật khẩu cho file văn bản trước khi gửi cho người khác là để đảm bảo thuộc tính nào của dữ liệu?
870. Tính sẵn sàng
871. Tính bí mật
872. Tính xác thực
873. Tính công khai
874. Tại sao cần có bước After khi triển khai an ninh dữ liệu?
875. Vì After là để duy trì trạng thái an ninh an toàn của hệ thống
876. Vì After là để thiết lập các biện pháp phòng thủ, phòng chống cho hệ thống
877. Vì con người hay bỏ qua bước Before và During
878. Vì các giải pháp phòng chống tấn công đôi khi không đủ an toàn 100%
879. Cài đặt phần mềm diệt Virus thuộc bước nào trong 3 bước triển khai an ninh dữ liệu?
880. Never
881. After
882. During
883. Before
884. Đâu không phải là một tổn thất khi mất an ninh dữ liệu?
885. Mất tính sẵn sàng
886. Tổn thất lòng tin
887. Tổn thất tài chính
888. Tổn thất tinh thần
889. Phương thức nào sau đây thuộc biện pháp an ninh dữ liệu vật lý (Physical)?
890. Khóa vân tay cho phòng làm việc﻿
891. Bảo vệ truy cập mạng Wifi công ty
892. Nội quy, quy định sử dụng máy tính an toàn
893. Cài đặt phần mềm diệt virus
894. Ba hiểm họa đối với dữ liệu trong bài bao gồm:
895. Thảm họa tự nhiên, người sử dụng, hiểm họa từ kẻ tấn công bên ngoài
896. Người sử dụng, người quản lý, người bên ngoài
897. Người bên trong tổ chức, đối thủ cạnh tranh, hacker tự do
898. Cái gì sau đây không phải là dữ liệu hữu hình?
899. File văn bản doc trên máy tính
900. Ảnh chụp gia đình
901. Hồ sơ dự thầu của công ty
902. Danh tiếng của công ty
903. Data Breach là gì?
904. Hỏng dữ liệu
905. Mất dữ liệu
906. Thất thoát dữ liệu
907. Thay đổi dữ liệu
908. Khi cần kiểm soát các kết nối mạng vào/ra máy tính cá nhân, bạn sẽ dùng chức năng nào trên Windows và Mac?
909. Anti Virus
910. Firewall
911. Google Chrome
912. Encryption
913. Tính năng EFS và Bitlocker trên Windows khác gì nhau?
914. EFS để mã hóa toàn bộ ổ cứng máy tính, còn Bitlocker dùng để mã hóa từng file/folder
915. EFS để mã hóa từng file/folder, còn Bitlocker dùng để mã hóa toàn bộ ổ cứng
916. EFS dùng để mã hóa còn Bitlocker dùng để chống mã độc
917. Bitlocker dùng để mã hóa còn EFS dùng để chống mã độc
918. Mật khẩu máy tính nào sau đây đủ mạnh?
919. Password
920. 66668888
921. M@tkha
922. Maytinhcuatoiratantoan
923. Nếu bạn có một thư mục chứa nội dung quan trọng và máy tính sử dụng chung cùng người khác, bạn nên làm gì để người khác không nhìn được thư mục này trên máy?
924. Mã hóa toàn bộ ổ cứng
925. Nâng mức cảnh báo an ninh cho hệ điều hành
926. Dùng chức năng Windows Firewall để chặn người khác không truy cập được file
927. Dùng chức năng ẩn file và folder
928. Chức năng mã hóa ổ cứng trên máy tính MacOS gọi là gì?
929. BitLocker
930. File encryptor
931. FileVault
932. MacVault
933. Vì sao cần khóa máy tính khi không sử dụng?
934. Để tiết kiệm điện
935. Để máy tính bền hơn
936. Để tránh người khác truy cập máy tính khi chúng ta không có mặt
937. Để chống mã độc xâm nhập từ Internet
938. Tính năng nào giúp hệ điều hành Windows cập nhật sửa lỗi phần mềm và các lỗ hổng bảo mật?
939. Windows Firewall
940. Windows Defender
941. Windows Update
942. indows Explorer
943. Tính năng nào của Windows giúp chống các Virus và Threat trên máy tính?
944. Windows Defender
945. Windows Firewall
946. Windows Malware
947. Windows Bitlocker
948. Tại sao cần mã hóa ổ cứng máy tính xách tay?
949. Để ngắt truy cập Internet của máy
950. Để nếu mất máy sẽ không bị lộ dữ liệu cho người khác
951. Để tránh bị mã độc tống tiền tấn công
952. Để bảo vệ dữ liệu không bị hỏng hóc
953. Tiêu chuẩn cơ bản nhất khi tiến hành Pentest Audit cho ứng dụng Web là:
     1. OWASP
     2. OWAPS
     3. WAPS
     4. OWAP
954. Đâu không phải là lỗ hổng bảo mật ứng dụng web?
     1. SQL Injection
     2. Broken Authentication
     3. SQL Enjection
     4. XSS (Cross Site Scripting)
955. Phát biểu nào dưới đây không phải là bảo mật thông tin trong hệ cơ sở dữ liệu?
     1. Ngăn chặn các truy cập không được phép
     2. Hạn chế tối đa các sai sót của người dùng
     3. Đảm bảo thông tin không bị mất hoặc bị thay đổi ngoài ý muốn
     4. Khống chế số người sử dụng CSDL
956. Theo bạn, đâu là phương pháp tiến hành đánh giá an toàn ứng dụng web?
     1. Black box
     2. Cả ba đáp án A, C, D
     3. White box
     4. Gray box
957. Theo bạn, đâu là phát biểu đúng nhất về quá trình đánh giá an toàn thông tin ứng dụng web?
     1. Xây dựng cấu trúc site, thư mục; Liệt kê tất cả điểm vào ứng dụng; Xác định khả năng tấn công; Kiểm tra lỗi chính tả; Kiểm tra lại bằng công cụ
     2. Xây dựng cấu trúc site, thư mục; Liệt kê tất cả điểm vào ứng dụng; Xác định khả năng tấn công; Kiểm tra lỗi; Kiểm tra lại bằng công cụ.
     3. Xây dựng cấu trúc Website, thư mục; Liệt kê tất cả điểm vào ứng dụng; Xác định khả năng tấn công; Kiểm tra lỗi; Kiểm tra lại bằng công cụ
     4. Xây dựng cấu trúc trường thông tin; Liệt kê tất cả điểm vào ứng dụng; Xác định khả năng tấn công; Kiểm tra lỗi; Kiểm tra lại bằng công cụ
958. Các mã lỗi CVE-2021-40471, CVE-2021-40473, CVE-2021-40374, CVE-2021-40479, CVE-2021-40485 là:
     1. Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.
     2. Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.
     3. Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.
     4. Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.
959. Các mã lỗi CVE-2021-40471, CVE-2021-40480, CVE-2021-40481 là:
     1. Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.
     2. Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.
     3. Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.
     4. Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.
960. Các mã lỗi CVE-2021-21572, CVE-2021-21573, CVE-2021-21574 là:
     1. Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.
     2. Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.
     3. Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.
     4. Lỗi tràn bộ đệm cho phép vượt qua các cơ chế kiểm soát để thực thi các đoạn mã độc hại với quyền người dùng quản trị. Khai thác được khi có quyền truy cập cục bộ.
961. Mã lỗi CVE-2021-36934 là:
     1. Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.
     2. Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa
     3. Lổ hổng bảo mật tồn tại do các tài khoản người dùng thường có thể truy cập vào các tệp hệ thống (như các tệp SAM, Windows Registry).
     4. Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.
962. Chọn đáp án đúng nhất. Theo bạn, sai sót trong cấu hình an ninh sẽ dẫn đến?
     1. Nguy cơ cho phép kẻ tấn công ngay lập tức tấn công DOS đối với hệ thống mạng.
     2. Nguy cơ cho phép kẻ tấn công không thể tìm hiểu rõ hệ thống mạng.
     3. Nguy cơ cho phép kẻ tấn công dễ dàng chiếm được tài khoản quản trị, quyền quản trị hệ thống từ đó chiếm quyền điều kiển máy chủ.
     4. Nguy cơ cho phép kẻ tấn công đồng thời sử dụng các công cụ tấn công tự động vào hệ thống mạng.
963. Chọn đáp án đúng nhất. Theo bạn, lưu trữ mật mã không an toàn sẽ dẫn đến?
     1. Nguy cơ cho phép kẻ tấn công dễ dàng chiếm được tài khoản quản trị, quyền quản trị hệ thống từ đó chiếm quyền điều kiển máy chủ.
     2. Nguy cơ khi hệ thống bị tấn công và kẻ tấn công lấy được thông tin trong cơ sở dữ liệu, các dữ liệu nhạy cảm sẽ bị lộ nếu không được mã hóa hoặc mã hóa không an toàn.
     3. Nguy cơ cho phép kẻ tấn công dễ dàng tấn công DOS vào hệ thống mạng.
     4. Nguy cơ cho phép kẻ tấn công dễ dàng rà quét mô phỏng chi tiết hệ thống mạng của victim.
964. Bạn nhận được email này, link này dẫn bạn đến đường link nào?

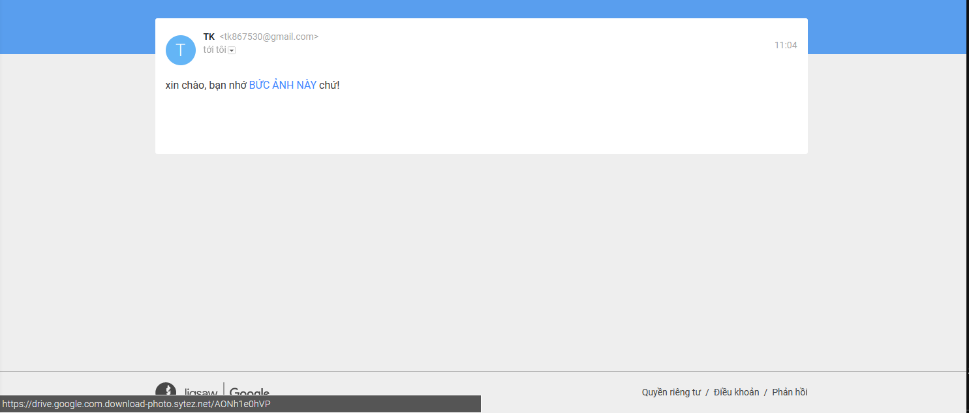
Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Chuyển đến tên miền giả mạo drive-google.com
2. Chuyển đến tên miền google drive
3. Chuyển đến tên miền mail.laocai.gov.vn
4. Không chuyển đến tên miền nào
5. Bạn nhận được email này, Đường liên kết thực sự chuyển đến tên miền nào dưới đây?



1. Đường liên kết thực sự chuyển đến mailru382.co
2. Đường liên kết thực sự chuyển đến hosting.com
3. Đường liên kết thực sự chuyển đến efacks.com
4. Không chuyển đến tên miền nào
5. Bạn nhận được email này, Khi bạn xem ảnh link đến tên miền thực sự là :



1. Tên miền google.com
2. Tên miền drive.google.com
3. Tên miền sytez.net
4. Không có tên miền liên kết
5. Bạn nhận được email này, Email này có phải lừa đảo không? Chọn đáp án đúng nhất

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Đây la email lừa đảo
2. Đây là email tin tưởng vì chuyển hướng đến <https://dropbox.com>
3. Đây là email tin lừa đảo vì đây có nội dung dropbox
4. Đây là email lừa đảo vì Giao diện giống dropbox
5. Bạn nhận được email này, Email này có phải lừa đảo không? Chọn đáp án đúng nhất

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Đây là Email tin tưởng
2. Đây có thể Email lừa đảo, Các tệp PDF có thể chứa phần mềm độc hại hoặc vi-rút
3. Đây có thể là Email tin tưởng do có file đính kèm .pdf
4. Đây có thể là Email tin tưởng do có Nội dung phù hợp
5. Bạn nhận được email này, Email này có phải lừa đảo không? Chọn đáp án đúng nhất

Ảnh có chứa văn bản

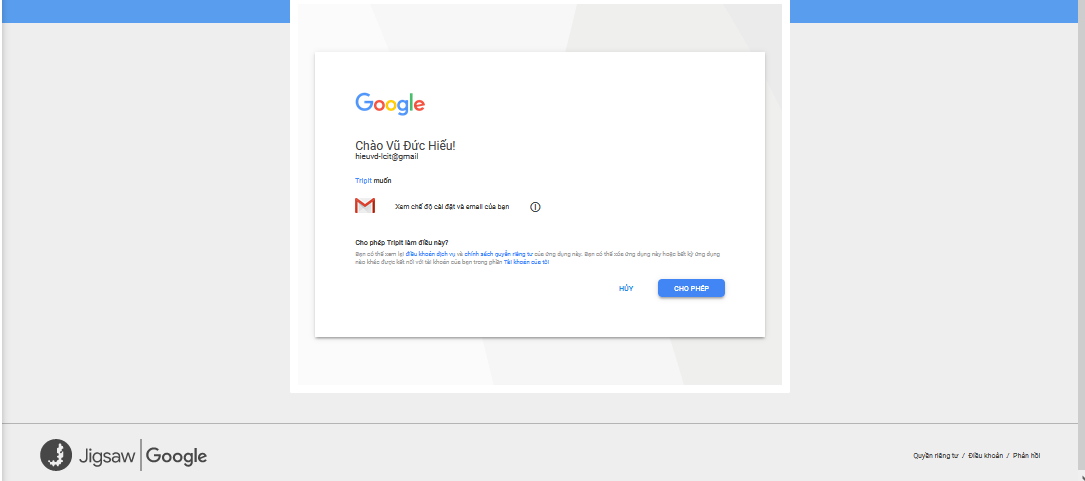
Mô tả được tạo tự động

1. Đây là Email lừa đảo do liên kết đến tên miền ml-Security.org
2. Đây là Email tin tưởng do từ google gửi
3. Đây là Email tin tưởng do có giao diện giống google
4. Đây là Email do Sở Thông tin Truyền thông gửi
5. Bạn nhận được email này, Email này có phải lừa đảo không? Chọn đáp án đúng nhất

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Đây là email xác thực từ google
2. Đây là email lừa đảo do Tin tặc đã tìm cách sử dụng Google để che giấu đường liên kết thực sự là từ tinyur
3. Đây là Email xác thực do có giao diện giống Google
4. Đây là Email do Sở Thông tin và Truyền thông gửi
5. Bạn nhận được email để google quét Email của mình. Chọn đáp án đúng nhất?



1. Đây là Email có nội dung xác thực
2. Đây là Email lừa đảo do có giao diện giống Google
3. Đây là Email lừa đảo do có IP không phải của Google
4. Đây là Email Sở Thông tin và Truyền thông gửi
5. Sự khác nhau cơ bản giữa vmware- xen- open VZ
6. Vmware có chức năng tốt hơn so với 2 máy chủ kia
7. Máy ảo Open VZ hoạt động chương trình phụ thuộc vào cấu hình của máy.
8. Tốc độ xử lý của 3 máy như nhau.
9. Open VZ hoạt động dựa trên nhân Linux và hệ điều hành
10. Ưu điểm của Xen là gì ?
11. Cho phép lưu trữ nhiều các môi trường ảo (VE Aka) trên một máy chủ duy nhất.
12. Công nghệ ảo hóa thực sự cho phép chạy cùng lúc nhiều máy chủ ảo VPS trên 1 máy chủ vật lý.
13. Có thể lưu trạng thái của máy ảo tại từng thời điểm.
14. Có nhiều phiên bản chạy trên hầu hết các hệ điều hành để lựa chọn.
15. Ảo hóa xen có bao nhiêu phiên bản chính
16. 1
17. 2
18. 3
19. 4
20. File virus lây lan bằng phương pháp “Chèn đầu” áp dụng đối với file dạng nào sau đây?
21. File .Com
22. File .Exe
23. File .Bin
24. File.Tar
25. Phương thức nào sau đây là một trong những phương pháp lây nhiễm của virus Macro?
26. Tìm những vùng trống trong file rồi ghi đè mã của nó vào.
27. Lây nhiễm từ các mạng xã hội
28. Thông qua thành phần VBProject của các đối tượng Microsoft Office
29. Lây nhiễm từ người phục vụ mạng đến khách hàng
30. Các phương pháp lây nhiễm của Virus Trojan?
31. Lây nhiễm từ các mạng xã hội
32. Lây nhiễm từ file đính kèm trong mail
33. a và b đều đúng
34. a và b đều sai
35. Phương thức nào sau đây là một trong những phương pháp lây nhiễm của virus Macro?
36. Tìm những vùng trống trong file rồi ghi đè mã của nó vào.
37. Lây nhiễm từ các mạng xã hội
38. Thông qua thành phần VBProject của các đối tượng Microsoft Office
39. Lây nhiễm từ người phục vụ mạng đến khách hàng
40. Ảo hóa mức hệ điều hành còn gọi là:
41. Containers Virtualization hay Isolation
42. Hypervisor
43. Virtualization layer
44. Full Virtualization hay Paravirtualization
45. Máy ảo khách chạy trên Xen được gọi là:
46. Domains
47. Containers
48. Virtual PC
49. Console
50. Đâu không phải là ưu điểm của VMware:
51. Tính linh hoạt trong công việc.
52. Bảo mật tốt
53. Khai thác triệt để sức mạnh của công nghệ phần cứng.
54. Mã nguồn mở vì được xây dựng dựa trên nhân Linux.
55. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như: web server, FTP server, email server?

|  |  |
| --- | --- |
| 1. DMZ 2. VLAN | 1. VPN 2. Intranet |

1. Bạn hãy chỉ ra thứ tự có hệ số bảo mật từ cao đến thấp khi cấu hình các lớp mạng cho một cơ quan, doanh nghiệp, tổ chức?

|  |  |
| --- | --- |
| 1. LAN, WAN, Internet, DMZ 2. Internet, WAN, DMZ, LAN | 1. LAN, WAN, DMZ, Internet 2. DMZ, LAN, WAN, Internet |

1. Để biết được địa chỉ IP cổng Internet bạn đang dùng có nằm trong danh sách nạn nhân của các chiến dịch tấn công mạng, botnet... trong 30 ngày gần nhất. Bạn sẽ vào đâu để kiểm tra nhanh nhất?
   1. <https://ais.gov.vn>
   2. <https://khonggianmang.vn>
   3. <http://antoanthongtin.vn>
   4. <http://vncert.gov.vn>
2. Theo bạn phát biểu nào sau đây là sai khi nói về chữ ký số?
   1. Không có chứng thư số cho thiết bị, dịch vụ, phần mềm
   2. Có chứng thư số cho cá nhân
   3. Có chứng thư số cho cá nhân, cơ quan, tổ chức
   4. Đáp án B, C đúng
3. Khi người dùng tại cơ quan/đơn vị/địa phương bạn truy cập vào các phần mềm dùng chung của tỉnh đều bị chậm, theo bạn nguyên nhân thường do đâu?
   1. Máy chủ cài đặt phần mềm dùng chung của tỉnh có cấu hình thấp
   2. Cổng Internet phía các máy chủ cài đặt phần mềm dùng chung có băng thông thấp
   3. Băng thông Internet phía người dùng có thể bị nghẽn
   4. Đáp án A, B
4. Theo bạn, đâu là phần mềm hiện không còn được nhà cung cấp hỗ trợ cập nhật bản vá bảo mật?
   1. Đáp án B, C đúng
   2. Microsoft SQL Server 2008
   3. Microsoft Internet Explorer 10
   4. Microsoft Office 2010
5. Để thực hiện việc cập nhật bản vá cho các máy chủ đặt trong vùng không được phép kết nối trực tiếp với Internet, bạn sẽ lựa chọn giải pháp nào sau đây?
   1. Sử dụng phần mềm WSUS Offline Update
   2. Sử dụng phần mềm Windows Server Update Services (WSUS)
   3. Sử dụng phần mềm Windows Server
   4. Có thể sử dụng giải pháp A hoặc B
6. Để nâng cao công tác bảo đảm an toàn thông tin, bạn được cơ quan giao nhiệm vụ đề xuất lựa chọn mua sắm phần mềm Microsoft Office bảo đảm đến năm 2021 vẫn được hãng hỗ trợ cập nhật bản vá, bạn sẽ lựa chọn phần mềm phiên bản nào dưới đây?
7. Microsoft Office 2010
8. Microsoft Office 2020
9. Microsoft Office 365
10. Có thể lựa chọn B và C
11. Theo Luật An ninh mạng năm 2018 thì Tài khoản số là thông tin dùng để làm gì?
12. Chứng thực, xác thực, bảo đảm, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.
13. Chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.
14. Phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.
15. Xác thực để sử dụng thông tin và các dịch vụ trên không gian mạng, được cơ quan có thẩm quyền số hóa.
16. Theo Luật An ninh mạng năm 2018 thì Tài khoản số là thông tin dùng để làm gì?
17. Chứng thực, xác thực, bảo đảm, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.
18. Chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.
19. Phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.
20. Xác thực để sử dụng thông tin và các dịch vụ trên không gian mạng, được cơ quan có thẩm quyền số hóa.
21. Người có hành vi vi phạm được quy định trong Luật An ninh mạng thì bị xử lý như thế nào?
22. Tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường.
23. Tùy theo tính chất, mức độ vi phạm mà bị khiển trách, xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường .
24. Nhẹ thì bị xử lý vi phạm hành chính, nặng thì bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường.
25. Có thể bị buộc thôi việc, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường
26. Cơ quan nào có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương?
27. Bộ, ngành, cơ quan, tổ chức .
28. Ủy ban nhân dân cấp tỉnh.
29. Ủy ban nhân dân cấp huyện.
30. Ủy ban nhân dân cấp xã.
31. Hệ thống thông tin quan trọng về an ninh quốc gia trừ thông tin quân sự và thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ do ai thẩm định?
32. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.
33. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.
34. Ban Cơ yếu Chính phủ.
35. Tất cả các đáp án trên
36. Có bao nhiêu hành vi bị nghiêm cấm về an ninh mạng?
37. 5
38. 6
39. 7
40. 8
41. Virus lây lan trước khi hệ điều hành được nạp là virus nào sau đây?
42. Virus Trojan
43. Sâu Internet
44. Boot virus
45. File virus
46. Phương thức nào sau đây là một trong những phương pháp lây nhiễm của virus Macro?
47. Tìm những vùng trống trong file rồi ghi đè mã của nó vào.
48. Lây nhiễm từ các mạng xã hội
49. Thông qua thành phần VBProject của các đối tượng Microsoft Office
50. Lây nhiễm từ người phục vụ mạng đến khách hàng
51. Ảo hóa mức hệ điều hành còn gọi là:
52. Containers Virtualization hay Isolation
53. Hypervisor
54. Virtualization layer
55. Full Virtualization hay Paravirtualization
56. Máy ảo khách chạy trên Xen được gọi là:
57. Domains
58. Containers
59. Virtual PC
60. Console
61. Đâu không phải là ưu điểm của VMware:
62. Tính linh hoạt trong công việc.
63. Bảo mật tốt
64. Khai thác triệt để sức mạnh của công nghệ phần cứng.
65. Mã nguồn mở vì được xây dựng dựa trên nhân Linux.
66. Theo bạn, đâu là cổng dịch vụ mặc định của dịch vụ SMTP?

|  |  |
| --- | --- |
| 1. 21 2. 22 | 1. 23 2. 25 |

1. Trong các địa chỉ IP dưới đây, theo bạn đâu là địa chỉ riêng (Private IP) chỉ dùng định danh trong mạng riêng của cơ quan, tổ chức, doanh nghiệp?

|  |  |
| --- | --- |
| 1. 117.117.117.1 2. 118.118.118.1 | 1. 119.119.119.1 2. 10.10.10.1 |

1. Bạn muốn kiểm tra kết nối giữa hai máy tính trong cùng mạng cục bộ (LAN), lệnh nào sau đây đáp ứng yêu cầu của bạn?

|  |  |
| --- | --- |
| 1. IPCONFIG 2. PING | 1. TELNET 2. HOST |

1. Để triển khai một website trong mạng cục bộ của một cơ quan với tên miền WEB.EGOV.VN, theo bạn cần sử dụng máy chủ nào?

|  |  |
| --- | --- |
| 1. DHCP Server 2. Firewall Server | 1. DNS Server 2. File Server |

1. Hypervisor không thể là:
2. Phần cứng
3. Phần mềm
4. Một bản firmware
5. Một hệ thống mạng(network)
6. Tấn Công DOS Nhằm Mục Đích Gì?
7. Đánh cắp tài nguyên.
8. Không làm gì cả.
9. Phá hủy tài nguyên .
10. Xâm nhập và chiếm quyền điều khiển hệ thống
11. DDOS là viết tắt của từ nào?
12. Disable Denial of Service.
13. Deny Denial of Service.
14. Decription Denial of Service.
15. Distributed Denial of Service
16. Theo bạn phát biểu nào sau đây là đúng khi nói về chữ ký số?
17. Có thể ký số trên văn bản giấy
18. Có thể ký số trên tệp tin Microsoft Powerpoint
19. B, D đều đúng
20. Chỉ có thể ký số trên những loại tệp tin được truyền, đưa trên môi trường mạng
21. Kali Linux là bản phân phối Linux được sử dụng để
22. Penetration Testing
23. Networking Ping
24. OS Report
25. Account Manage
26. Để vào chế độ Enter Privilege mode (vào chế độ đặc quyền) sử dụng lệnh nào dưới đây:
27. Switch>enable
28. Switch#enable
29. Switch>enable mode
30. Switch# enable mode
31. Các loại switch phổ biến thường dùng
32. Layer 2 và Layer 3
33. Layer 1 và Layer 2
34. Layer 3 và Layer 4
35. Layer 1 và Layer 3
36. Authentication server là gì?
37. Là máy chủ xác thực quyền truy cập dùng các kỹ thuật xác thực mạnh
38. Là máy chủ cấp phát địa chỉ IP động
39. Là máy chủ cài đặt phần mềm Authentication
40. Là máy chủ Author
41. DMZ là gì?
42. Là vùng có nguy cơ bị tấn công từ Internet
43. Là vùng mạng kết nối các mạng LAN với nhau
44. Là vùng mạng nằm ngoài Internet
45. Là vùng thực thi các cơ chế bảo mật
46. Tên phần mềm giúp ngăn chặn kết nối tới máy chủ của kẻ tấn công, phần lớn các mã độc nguy hiểm có kết nối đến máy chủ điều khiển, mã hóa tống tiền, ...
47. ViSafe
48. Vesafe
49. Visave
50. ViProtect
51. Chứng chỉ nào dưới đây là chứng chỉ bảo mật
52. CEH
53. ECH
54. HEC
55. MOS
56. Hệ thống thông tin quan trọng về an ninh quốc gia bao gồm?
57. Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng .
58. Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái.
59. Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí .
60. Tất cả các đáp án trên
61. Máy tính A có địa chỉ IP 10.118.169.25 / 16. Trên máy tính A thực thi câu lệnh “ping 203.162.0.186” và nhận thông báo “Destination host unreachable”. Giải thích (các) nguyên nhân.
62. Không có Default Gateway
63. Có Default Gateway
64. Địa chỉ IP sai
65. Subnet của máy tính A sai
66. Để chuyển sang một thư mục khác ta dùng lệnh
67. Lệnh cdir
68. Lệnh cd
69. Lệnh mkdir
70. Lệnh dir
71. Để chép một file /tmp/hello.txt vào thư mục /tmp/hello/ ta phải làm lệnh nào sau đây
72. copy /tmp/hello.txt /tmp/hello/
73. cp tmp/hello.txt /tmp/hello
74. cp /tmp/hello /tmp/hello
75. cp /tmp/hello.txt /tmp/hello
76. Theo bạn, phát biểu nào sau đây đúng nhất khi nói về thiết bị chuyển mạch (Switch)?
77. Kết nối các máy tính trong mạng cục bộ (LAN)
78. Kết nối các máy tính trong mạng diện rộng cách xa nhau về mặt địa lý
79. Hoạt động từ lớp 1 đến lớp 7 trong mô hình OSI
80. Được thiết kế để hoạt động tại lớp 3 trong mô hình OSI
81. Theo bạn, đâu là cổng dịch vụ mặc định của dịch vụ SMTP?

|  |  |
| --- | --- |
| 1. 21 2. 22 | 1. 23 2. 25 |

1. Trong các địa chỉ IP dưới đây, theo bạn đâu là địa chỉ riêng (Private IP) chỉ dùng định danh trong mạng riêng của cơ quan, tổ chức, doanh nghiệp?

|  |  |
| --- | --- |
| 1. 117.117.117.1 2. 118.118.118.1 | 1. 119.119.119.1 2. 10.10.10.1 |

1. Bạn muốn kiểm tra kết nối giữa hai máy tính trong cùng mạng cục bộ (LAN), lệnh nào sau đây đáp ứng yêu cầu của bạn?

|  |  |
| --- | --- |
| 1. IPCONFIG 2. PING | 1. TELNET 2. HOST |

1. Để triển khai một website trong mạng cục bộ của một cơ quan với tên miền WEB.EGOV.VN, theo bạn cần sử dụng máy chủ nào?

|  |  |
| --- | --- |
| 1. DHCP Server 2. Firewall Server | 1. DNS Server 2. File Server |

1. Quota được dùng để…
2. Hiển thị việc sử dụng không gian lưu trữ
3. Giới hạn không gian lưu trữ
4. A và B đều đúng
5. Tất cả đều sai
6. Cơ quan bạn có một máy chủ đã được cài sẵn hệ điều hành Windows Server 2012, để cài đặt một website viết bằng PHP, theo bạn cần phải sử dụng phần mềm nào để cài đặt website này lên máy chủ?

|  |  |
| --- | --- |
| 1. DNS 2. IIS hoặc Apache | 1. Visual Studio 2. NET Framework |

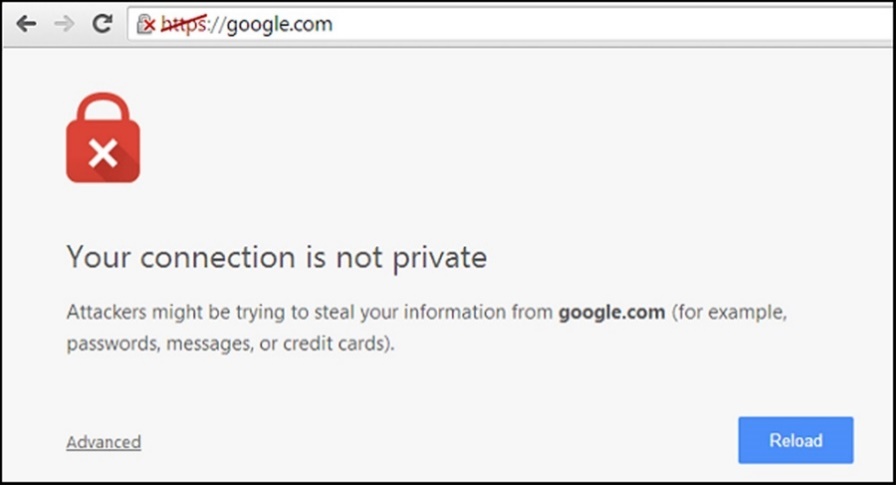
1. Chọn đáp án đúng nhất khi nói về mạng VLAN?
2. Là mạng dùng riêng ảo xác định trên mạng công cộng (public network)
3. Là mạng LAN ảo, xác định theo sơ đồ logic, không theo vị trí mạng vật lý
4. Là mạng cục bộ trong một tòa nhà
5. Là mạng diện rộng liên kết các mạng LAN trong khu vực rộng
6. Phương tiện vật lý nào cho khoảng cách xa nhất đối với mạng Ethernet?
7. Cáp quang đơn mode (Single-Mode)
8. Cáp quang đa mode (Multi-Mode)
9. Cáp đồng trục
10. Cáp xoắn đôi UTP
11. Theo bạn, Broadcast là gì?
12. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến một số điểm nhất định trong cùng một mạng
13. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến hầu hết các điểm khác trong cùng một mạng
14. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến tất cả các điểm khác trong cùng một mạng
15. Là thuật ngữ được sử dụng trong mạng máy tính để mô tả cách thức truyền tin được gửi từ 1 điểm đến tối đa 32 điểm khác trong cùng một mạng
16. 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 (ví dụ như Internet)?

|  |  |
| --- | --- |
| 1. Điểm truy cập không dây 2. Router | 1. Tường lửa 2. Switch |

1. Ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng ?

|  |  |
| --- | --- |
| 1. IDS 2. FTP | 1. Router 2. Sniffer |

1. 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?
2. 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
3. Mở chương trình và chạy nó ngay. Chương trình đó thật sự an toàn vì nó được gửi từ Microsoft
4. Xoá email đó ngay. Microsoft và các nhà cung cấp không bao giờ gửi chương trình sửa lỗi qua email.
5. Tất cả đều sai
6. Khi cung cấp kết nối không dây (Wi-Fi) trong cơ quan, đơn vị bạn. Việc chia tách phần mạng Wi-Fi riêng ở một lớp mạng khác để tăng tính bảo mật mạng, tại thiết bị AccessPoint bạn nên làm như thế nào?
7. Nối cổng WAN vào nút mạng bất kỳ của cơ quan, đơn vị
8. Nối cổng LAN vào nút mạng bất kỳ của cơ quan, đơn vị
9. Thiết lập tường lửa trên AccessPoint
10. Đặt mật khẩu truy cập trên AccessPoint
11. Để kiểm tra địa chỉ email của bạn có bị lộ lọt thông tin tài khoản không, bạn sẽ truy cập vào đâu để thực hiện điều này?
    1. <https://khonggianmang.vn/check-data-leak>
    2. Trang thông tin điện tử của Trung tâm giám sát an toàn không gian mạng quốc gia
    3. Website của nhà mạng
    4. Cả A và B đều được.
12. Khi duyệt web, nếu người dùng gặp phải lỗi như hình dưới đây, theo bạn đó là lỗi gì?



1. Máy tính người dùng đang sử dụng phiên bản Windows 7
2. Chứng chỉ bảo mật SSL hết hạn hoặc không tin cậy
3. Máy tính người dùng bị mã độc tấn công
4. Cả A và B đúng
5. DDOS là sự tấn công:
6. 1 cá nhân đánh hủy 1 hệ thống.
7. 1 vài cá nhân dánh hủy 1 hệ thống.
8. 1 cá nhân điều khiển nhiều máy zombie để phá hủy hệ thống.
9. Nhiều cá nhân đánh hủy 1 hệ thống.
10. Cơ quan nào có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương?
11. Bộ, ngành, cơ quan, tổ chức .
12. Ủy ban nhân dân cấp tỉnh.
13. Ủy ban nhân dân cấp huyện.
14. Ủy ban nhân dân cấp xã.
15. Hệ thống thông tin quan trọng về an ninh quốc gia trừ thông tin quân sự và thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ do ai thẩm định?
16. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.
17. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.
18. Ban Cơ yếu Chính phủ.
19. Tất cả các đáp án trên
20. Máy tính A có địa chỉ IP 172.18.1.25 / 16. Chọn các địa chỉ có thể là default gateway của máy tính A
21. 172.19.1.25
22. 172.19.1.255
23. 172.18.255.254
24. 172.18.251.256
25. Để liệt kê các file có trong thư mục hiện hành ta dùng lệnh:
26. Lệnh df
27. Lệnh ls
28. Lệnh du
29. Lệnh cp
30. Để liệt kê đầy đủ thông tin của các file có trong thư mục hiện hành theo ta dùng lệnh ls với tham số
31. –a
32. –l
33. –x
34. –n
35. Lệnh nào sau đây dùng để chuyển sang người dùng khác
36. #man
37. #hostName
38. #su
39. #vi
40. Mỗi thiết bị trong Linux là một tập tin lưu trong thư mục
41. /etc
42. /mnt
43. /home
44. /dev
45. Tập tin /etc/password chứa thông tin gì của users hệ thống
46. Chứa profile của người dùng
47. Chứa uid, gid, home directory, shell
48. Chứa password của người dùng
49. Chứa tập shadow của người dùng
50. [Chương trình soạn thảo nào sau đây không sử dụng giao diện đồ hoạ:](https://doctailieu.com/trac-nghiem/chuong-trinh-soan-thao-nao-sau-day-khong-su-dung-giao-dien-do-hoa-c-vi-trac-34828)
51. emacs
52. latex
53. vi
54. kword
55. [Trong vi, để vào mode edit insert ta phải dùng lệnh nào:](https://doctailieu.com/trac-nghiem/trong-vi-de-vao-mode-edit-insert-ta-phai-dung-lenh-nao-b-esc-i-trac-nghiem-34830)
56. Dùng phím F4
57. ESC-:i
58. ESC-:q
59. ESC-:x
60. [Để xem chi tiết các tiến trình đang chạy trong hệ thống ta dùng lệnh ps với các tham số nào sau đây](https://doctailieu.com/trac-nghiem/de-xem-chi-tiet-cac-tien-trinh-dang-chay-trong-he-thong-ta-dung-lenh-ps-voi-cac-34831)
61. –ef
62. –ax
63. –axf
64. Cả 3 câu đều đúng
65. [Mỗi tiến trình chạy trong hệ thống Linux được đặc trưng bởi:](https://doctailieu.com/trac-nghiem/moi-tien-trinh-chay-trong-he-thong-linux-duoc-dac-trung-boi-a-pid-trac-nghiem-34832)
66. PID
67. PUID
68. PGUID
69. GUID
70. [Để dừng một tiến trình ta dùng lệnh nào](https://doctailieu.com/trac-nghiem/de-dung-mot-tien-trinh-ta-dung-lenh-nao-b-kill-trac-nghiem-mon-quan-tri-he-34834)
71. stop
72. kill
73. shutdown
74. halt
75. [Để thiết lập địa chỉ IP cho một máy Linux ta sử dụng lệnh nào trong các lệnh sau đây:](https://doctailieu.com/trac-nghiem/de-thiet-lap-dia-chi-ip-cho-mot-may-linux-ta-su-dung-lenh-nao-trong-cac-lenh-sau-34837)
76. ipconfig
77. ifconfig
78. netstat
79. route
80. [Để thay đổi các lựa chọn gắn kết (mount) tự động cho một hệ thống tập tin cục bộ, ta cần sửa đổi nội dung tập tin nào?](https://doctailieu.com/trac-nghiem/de-thay-doi-cac-lua-chon-gan-ket-mount-tu-dong-cho-mot-he-thong-tap-tin-cuc-34843)
81. /etc/filesystems
82. /etc/fstab
83. /etc/group
84. /etc/mnttab
85. [Lệnh nào để xóa tập tin có tên là "-abc"](https://doctailieu.com/trac-nghiem/lenh-nao-de-xoa-tap-tin-co-ten-la-abc-c-rm-abc-trac-nghiem-mon-quan-tri-he-34847)
86. rm –f –abc
87. rm –i –abc
88. rm -- -abc
89. rm \ -abc
90. [Để khóa tài khoản "user", ta dùng lệnh?](https://doctailieu.com/trac-nghiem/de-khoa-tai-khoan-user-ta-dung-lenh-b-passwd-l-user-trac-nghiem-mon-quan-tri-34850)
91. usermod –L user
92. passwd –l user
93. A và B đều sai
94. A và B đều đúng
95. [Lệnh nào dùng để liệt kê danh sách tất cả các tập tin có tên phần mở rộng không chứa các ký tự trong khoảng từ "x" đến "w" trong thư mục hiện hành:](https://doctailieu.com/trac-nghiem/lenh-nao-dung-de-liet-ke-danh-sach-tat-ca-cac-tap-tin-co-ten-phan-mo-rong-khong-34855)
96. ls \*.!x | .!w
97. ls \*.[!x-w]
98. ls ! \*.[xz]
99. ls \*.[!xw]
100. [. Để tạo tài khoản người dùng "abc" là thành viên của nhóm "group", ta dùng lệnh:](https://doctailieu.com/trac-nghiem/de-tao-tai-khoan-nguoi-dung-abc-la-thanh-vien-cua-nhom-group-ta-dung-lenh-a-34856)
101. useradd –g group abc
102. useradd –G group abc
103. useradd –m group abc
104. useradd group abc
105. [Bạn sử dụng lênh sau useradd –m sapa song user sapa không đăng nhập vào được.Để đăng nhập được ta phải làm gì?](https://doctailieu.com/trac-nghiem/ban-su-dung-lenh-sau-useradd-m-sapa-song-user-sapa-khong-dang-nhap-vao-duocde-34857)
106. Cần đăng ký mật khẩu cho user sapa bằng lệnh password sapa
107. Phải tạo thư mục home cho sapa và tạo quyền cho phép truy cập.
108. Bạn cần biên tập lại file /etc/passwd và đăng ký shell cho acount sapa
109. Bạn cần biên tập lại file /etc/passwd và đăng ký shell cho acount sapa
110. [Mở file /etc/passwd ta thấy có các dòng .Trật tự nào sau đây của các trường là đúng:](https://doctailieu.com/trac-nghiem/mo-file-etc-passwd-ta-thay-co-cac-dong-trat-tu-nao-sau-day-cua-cac-truong-la-34858)
111. username, UID, GID, home directory, command, comment
112. username, UID, GID, comment, home directory, command
113. UID, username, GID, home directory, comment, command
114. username, UID, group name, GID, home directory, comment
115. [Quan sát file /etc/passwd , thấy trong trường password chứa ký hiệu "x’. Ý nghĩa của ký tự này là gì?](https://doctailieu.com/trac-nghiem/quan-sat-file-etc-passwd-ban-thay-trong-truong-password-chua-ky-hieu-x-b-34861" \o "Xem chi tiết câu hỏi)
116. Password đã được mã hoá.
117. Đang sử dụng shadow password.
118. Tất cả passwords đều rỗng.
119. Tất cả passwords đều hết hạn.
120. [Sau khi Hieu rời khỏi cơ quan ,bạn dùng lệnh userdel dung để xoá user này.Mẩu tin của user này trong file etc/passwd bị xoá , tuy vậy trong home directory có thể vẫn còn thư mục của user này. Bạn có thể dùng lệnh nào sau đây để khẳng định home directory cũng đã bị xoá?](https://doctailieu.com/trac-nghiem/sau-khi-dung-roi-khoi-cong-ty-ban-dung-lenh-userdel-dung-de-xoa-user-naymau-34862)
121. userdel –m hieu
122. userdel –u hieu
123. userdel –l hieu
124. userdel –r hieu
125. [Tập tin sau đây có thuộc tính như thế nào:  
     -rwx--x--x hello.sh](https://doctailieu.com/trac-nghiem/tap-tin-sau-day-co-thuoc-tinh-nhu-the-nao-d-711-trac-nghiem-mon-quan-tri-he-34799)
126. 077
127. 644
128. 755
129. 711
130. Theo bạn, đâu là cổng dịch vụ mặc định của dịch vụ DNS?

|  |  |
| --- | --- |
| 1. 22 2. 52 | 1. 53 2. 553 |

1. Cho các địa chỉ IPv4 dưới đây, bạn hãy cho biết đâu là địa chỉ thuộc lớp A?

|  |  |
| --- | --- |
| 1. 10.118.168.1 2. 192.168.0.1 | 1. 172.168.0.1 2. 128.118.168.1 |

1. Lệnh nào sau đây cho biết địa chỉ IP của máy tính trong Windows?

|  |  |
| --- | --- |
| 1. IP 2. TCP\_IP | 1. IPCONFIG 2. HOST |

1. Trong các phần mềm dưới đây, theo bạn đâu là phần mềm ảo hóa có thể cài đặt được trên máy tính cá nhân (PC)?

|  |  |
| --- | --- |
| 1. VMWare Workstation 2. Visual Basic | 1. Microsoft Hyper-V 2. Cả A và C |

1. Cho địa chỉ mạng con (subnet): 192.168.2.0/24 bạn hãy cho biết, mạng này có thể định được tối đa bao nhiêu host?

|  |  |
| --- | --- |
| 1. 64 2. 128 | 1. 254 2. 255 |

1. Bạn muốn kết nối đến máy chủ trong LAN của cơ quan để thực hiện một số tác vụ quản trị máy chủ từ xa, bạn sẽ sử dụng lệnh nào sau đây?

|  |  |
| --- | --- |
| 1. TRACERT 2. IPCONFIG | 1. TELNET 2. CONNECT |

1. Để cấp địa chỉ IP trong LAN, người ta sử dụng dịch vụ có giao thức nào?

|  |  |
| --- | --- |
| 1. DNS 2. DHCP | 1. SMTP 2. HTTP |

1. Theo bạn, thiết bị nào sau đây giúp định tuyến gói tin giữa các lớp mạng khác nhau trong hệ thống LAN của một cơ quan, tổ chức?

|  |  |
| --- | --- |
| 1. Switch layer 2 2. Swictch layer 3 | 1. Router 2. Cả B và C đều được |

1. Theo bạn, thiết bị nào sau đây giúp định tuyến gói tin giữa các lớp mạng khác nhau trong hệ thống LAN của một cơ quan, tổ chức?

|  |  |
| --- | --- |
| 1. Switch layer 2 2. Swictch layer 3 | 1. Router 2. Cả B và C đều được |

1. Trình tự đóng gói dữ liệu khi truyền từ máy A đến máy B là?

|  |  |
| --- | --- |
| 1. Data, packet, segment, frame, bit. 2. Data, frame, packet, segment, bit | 1. Data, segment, frame, packet, bit. 2. Data, segment, packet, frame, bit. |

1. Tiêu chuẩn cho mạng không dây Wi-Fi là tiêu chuẩn nào sau đây?

|  |  |
| --- | --- |
| 1. IEEE 802.2 2. IEEE 802.3 | 1. IEEE 802.11 2. IEEE 802.16 |

1. Cho mạng con 172.16.0.0/22, theo bạn địa chỉ nào không là địa chỉ host thuộc mạng này?

|  |  |
| --- | --- |
| 1. 172.16.1.254 2. 172.16.2.254 | 1. 172.16.3.254 2. 172.16.4.254 |

1. Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm hệ điều hành?
2. Cài đặt bản service pack mới nhất
3. Cài đặt lại HĐH thông dụng
4. Sao lưu hệ thống thường xuyên
5. Shut down hệ thống khi không sử dụng
6. Một người dùng vừa mua phải một máy tính xách tay đã nhiễm virus, trên máy không chứa phần mềm Antivirus và chưa được kết nối với mạng. Theo bạn, cách tốt nhất để xử lý máy tính xách tay này là gì?
7. Nối mạng máy tính xách tay và download phần mềm antivirus từ máy chủ
8. Khởi động máy tính xách tay với đĩa khởi động Antivirus mới nhất
9. Nối mạng máy tính xách tay và download phần mềm Antivirus từ Internet
10. Kết nối máy tính xách tay đến một máy tính cá nhân khác và diệt virus từ đó
11. “An ninh mạng” là gì?

A) Là sự giám sát hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân..

B) Là sự kiểm tra hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

C) Là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

D) Là sự phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

1. Hệ thống thông tin quan trọng về an ninh quốc gia bao gồm?
2. Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng .
3. Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái.
4. Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí
5. Tất cả các đáp án trên.
6. You want to establish a network connection between two LANs using the Internet. Which technology would best accomplish that for you?
7. IPSec
8. L2TP
9. PPP
10. SLIP
11. Which kind of attack is designed to overload a particular protocol or service?
12. Spoofing
13. Back door
14. Man in the middle
15. Flood
16. What is the process of making an operating system secure from attack called (choose the best answer)?
17. Hardening
18. Tuning
19. Sealing
20. Locking down
21. The integrity objective addresses which characteristic of information security?
22. Verification that information is accurate
23. Verification that ethics are properly maintained
24. Establishment of clear access control of data
25. Verification that data is kept private and secure
26. The mechanism or process is used to enable or disable access to a network resourcebased on an IP address?
27. NDS
28. ACL
29. Hardening
30. Port blocking
31. What type of program exists primarily to propagate and spread itself to other systems?
32. Virus
33. Trojan horse
34. Logic bomb
35. Worm
36. An individual presents herself at your office claiming to be a service technician. She wants to discuss your current server configuration. This may be an example of what type of attack?
37. Social engineering
38. Access control
39. Perimeter screening
40. Behavioral engineering
41. What encryption process uses one message to hide another?
42. Steganography
43. Hashing
44. MDA
45. Cryptointelligence
46. Which of the following types of logs could provide clues that someone has been attempting to compromise the SQL Server database?
47. Event
48. SQL\_LOG
49. Security
50. Access
51. Which of the following devices is the most capable of providing infrastructure security?
52. Hub
53. Switch
54. Router
55. Modem
56. Which protocol is primarily used for network maintenance and destination information?
57. ICMP
58. SMTP
59. IGMP
60. Router
61. Which device monitors network traffic in a passive manner?
62. Sniffer
63. IDS
64. Firewall
65. Web browser
66. Which technology allows a connection to be made between two networks using a secure protocol?
67. Tunneling
68. VLAN
69. Internet
70. Extranet
71. What should a VPN over wireless use for tunneling?
72. TKIP
73. SSL or IPSec
74. CCMP
75. PEAP
76. You want to assign privileges to a user so that she can delete a file but not be able to assign privileges to others. What permissions should you assign?
77. Full Control
78. Delete
79. Administrator
80. Modify
81. Which of the following does not apply to a hashing algorithm?
82. One-way
83. Long key size
84. Variable-length input with fixed-length output
85. Collision resistance
86. Which of the following is the most widely used asymmetric algorithm today?
87. RSA
88. AES
89. 3DES
90. SHA
91. You need to encrypt your hard drive. Which of the following is the best choice?
92. DES
93. RSA
94. AES
95. SHA
96. As the security administrator for your organization, you must be aware of all types of attacks that can occur and plan for them. Which type of attack uses more than one computer to attack the victim?
97. DoS
98. DdoS
99. Worm
100. UDP attack
101. An alert signals you that a server in your network has a program running on it that bypasses authorization. Which type of attack has occurred?
102. DoS
103. DdoS
104. Backdoor
105. Social engineering
106. Which type of attack denies authorized users access to network resources?
107. DoS
108. Worm
109. Logic bomb
110. Social engineering
111. What is it known as when an attacker manipulates the database code to take advantage of aweakness in it?
112. SQL tearing
113. SQL manipulation
114. SQL cracking
115. SQL injection
116. Which of the following is not part of the CIA triad?
117. Avoidance
118. Confidentiality
119. Availability
120. Integrity
121. Which of the following best defines social engineering?
122. Illegal copying of software
123. Gathering information from discarded manuals and printouts
124. Using people skills to obtain proprietary information
125. Destroying or altering data
126. Which attack belongs to LAN attacks?
127. ARP poinsoning
128. STP
129. DHCP rouge
130. VLAN hopping
131. TCP flood
132. Which encryption technology is associated with WPA?

A) TKIP

B) CCMP

C) WEP

D) LDAP

1. When a hole is found in a web browser or other software, and attackers begin exploiting it the very day it is discovered by the developer, what type of attack is it known as?

A) Polymorphic

B) Xmas

C) Malicious insider

D) Zero-day

1. What are the three most fundamental goals of computer security ?
2. Confidentiality
3. Auditing
4. Integrity
5. Privilege management
6. Availability
7. What is an example of a "what you do" authentication factor ?
8. Fingerprint or handprint recognition
9. ID card and PIN
10. Keystroke pattern recognition
11. Geolocation
12. Use name and password
13. In which of the following mobile connection methods does a receiver require an unobstructed view of the sender ?
14. Near-field communication (NFC)
15. Infrared
16. Bluetooth
17. SATCOM