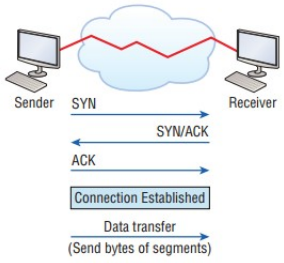
AN NINH MÁY TÍNH

A. Ôn tập trắc nghiệm

1. Hầu hết Mỗi host trên đường mạng TCP/IP phải được cấu hình cái gì nhằm để giao tiếp với các host khác
    a. Preferred WINS server
    b. Default gateway
    c. DHCP
    d. Preferred DNS server
2. Chiều dài tối thiểu của mật khẩu cần phải là:
    a. 12 đến 15 ký tự
    b. 3 đến 5 ký tự
    c. 8 ký tự
    d. 1 đến 3 ký tự
3. Câu hỏi: Mô hình TCP/IP có mấy lớp?
    a. 4 Lớp
    b. 5 Lớp
    c. 6 Lớp
    d. 7 Lớp
4. Câu hỏi: Địa chỉ IPv4 tổng cộng có bao nhiêu bit?
    a. 30 bit
    b. 31 bit
    c. 32 bit
    d. 33 bit
5. Câu hỏi: Địa chỉ IPv6 tổng cộng có bao nhiêu bit?
    a. 64 bit
    b. 128 bit
    c. 192 bit
    d. 256 bit
6. Địa chỉ IP 255.255.255.255 đại diện cho …….. trong bảng IP routing?
    a. Địa chỉ loopback
    b. Địa chỉ giới hạn broadcast
    c. Default route
    d. Đường route network gắn liền trực tiếp
7. Câu: Trong sơ đồ dưới đây, quy trình nào được thể hiện?



a. flow control
b. **TCP handshake**
c. Windowing
d. reliable delivery

8. Câu hỏi: Cờ TCP nào sau đây được sử dụng để đóng kết nối không cần xác nhận?
   a. ACK
   b. RST
   c. PSH
   d. FIN
9. Giao thức lớp Ứng dụng nào sau đây thiết lập phiên bảo mật tương tự như Telnet?
   a. FTP
   b. DNS
   c. DHCP
   d. SSH
10. Tấn công từ chối dịch vụ nhằm tấn công tính:
   a. **Sẵn dùng (Availability)**
   b. Tin cậy (Confidentiality)
   c. Không từ chối (Non-repudiation)
   d. Toàn vẹn (Integrity
11. Nguyên tắc nào sau đây bị vi phạm nếu hệ thống máy tính không thể truy cập được?
   a. Sẵn dùng (Availability)
   b. Tin cậy (Confidentiality)
   c. Không từ chối (Non-repudiation)
   d. Toàn vẹn (Integrity
12. Chứng nhận chứa:
   a. Chữ ký
   b. Thông tin thuật toán tạo mã khoá
   c. Thuật toán tạo chữ ký
   d. Tất cả đều đúng
13. Điều nào sau đây không phải là một mục tiêu chính của an ninh máy tính?
   a. Đảm bảo sự sẵn có của dữ liệu công ty
   b. Duy trì tính toàn vẹn của dữ liệu công ty
   c. Bảo vệ chống lại tấn công từ chối dịch vụ tấn công
   d. Bảo vệ tính bảo mật của dữ liệu công ty
14. Trong mật mã, khóa công khai dùng để làm gì?
   a. Mã hóa
   b. Giải mã
   c. Kí
   d. Kiểm tra chữ ký
15. Trong mật mã, khóa bí mật dùng để làm gì?
   a. Mã hóa

b. Giải mã
c. Kí
d. Kiểm tra chữ ký

16. Trong sơ đồ ký số thành phần nào đặc trưng xác nhận cho một người?
    a. Khóa công khai
    b. Khóa bí mật
    c. Bản mã
    d. Bức điện
17. Nếu ta muốn xác thực chữ ký của một người khác, khóa nào phải được sử dụng?
    a. Khóa công khai của bạn
    b. Khoá cá nhân của bạn
    c. Khoá cá nhân của người cần xác thực
    d. Khoá công khai của người cần xác thực
18. Hệ mã thỏa điều kiện với mấy bộ:
    a. 2
    b. 3
    c. 4
    d. 5
19. Hệ mã Des mã hóa với bao nhiêu bit
    a. 56
    b. 64
    c. 128
    d. 192
20. Giao thức nào sử dụng cả UDP và TCP ports?
    a. SMTP
    b. Telnet
    c. FTP
    d. DNS
21. Các tập tin nào sau đây có khả năng chứa virus nhất?
    a. database.dat
    b. bigpic.jpeg
    c. note.txt
    d. picture.gif.exe
22. Tầng nào trong các tầng sau của mô hình OSI cung cấp chức năng mã hóa?
    a. Application
    b. Presentation
    c. Session
    d. Data Link Layer
23. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và giải mã?
    a. Không đối xứng
    b. Đối xứng
    c. RSA

d. Diffie-Hellman

24. Chữ ký số được sử dụng cho mục đích gì?
    a. Để bảo mật tài liệu sao cho người ngoài không đọc được
    b. Để kiểm tra định danh người gửi
    c. Cung cấp chứng chỉ
    d. Thu hồi một chứng chỉ
25. Phân loại mức độ thông tin nào sau đây có độ an toàn cao nhất?
    a. Confidential
    b. Public
    c. Private
    d. Sensitive
26. Thực thể nào sau đây cho phép phát hành , quản lý, và phân phối các chứng chỉ số ?
    a. Quyền cấp chứng chỉ (Certificate Authority)
    b. Quyền đăng ký (Registration Authority)
    c. Chính phủ (NSA)
    d. PKI
27. Hệ mật DES sử dụng khối khóa được tạo bởi :
    a. 56 bit ngẫu nhiên
    b. 64 bit ngẫu nhiên
    c. 128 bit ngẫu nhiên
    d. 56 bit ngẫu nhiên và 8 bit kiểm tra "Parity"
28. Một địa chỉ IP có thể được gán cho một card mạng Internet?
    a. 192.168.20.223
    b. 172.16.200.18
    c. 10.180.48.224
    d. 9.255.255.10
29. Trong DoD, ICMP nằm ở tầng nào?
    a. Application
    b. Host to host
    c. Internet
    d. Network Access
30. Trên mạng 131.1.123.0/27, địa chỉ IP cuối cùng có thể được gán cho một host là gì?
    a. 131.1.123.30
    b. 131.1.123.33
    c. 131.1.123.31
    d. 131.1.123.32
31. Câu nào bên dưới định nghĩa malware đúng nhất? (chọn 2)
    a. Malware là một dạng virus
    b. Trojans là malware
    c. Malware chứa tất cả phần mềm độc hại (malicious software)
    d. Malware chỉ bao gồm phần mềm gián điệp

32. Điều nào sau đây là đúng của một worm? (chọn 2)
    a. Worm là phần mềm độc hại
    b. Worm có khả năng tự sao chép
    c. Worm tự sao chép với tương tác người dùng
    d. Worm là chương trình chạy âm thầm
33. SSL do ai phát triển?
    a. Microsoft
    b. Netscape
    c. RSA
    d. Verisign
34. Giai đoạn đầu tiên của hacker là gì?
    a. Maintaining access
    b. Scanning
    c. Gaining access
    d. Reconnaissance
35. Thuật giải SHA là :
    a. Hàm băm một chiều
    b. Dùng trong thuật giải tạo chữ ký số
    c. Cho giá trị băm 160 bit
    d. **Tất cả đều đúng**
36. Loại hacker nào gây ra sự rủi ro cao nhất cho hệ thống mạng:
    a. Disgruntled employees
    b. Black-hat hackers
    c. Grey-hat hackers
    d. Script kiddies
37. Hệ thống nào sau đây có thể được sử dụng để giám sát một mạng đối với các hành động trái phép ?
    a. Network sniffer
    b. N-IDS (Network-based IDS)
    c. A và B đều sai
    d. A và B đều đúng
38. Hệ thống nào được cài đặt trên Host để cung cấp một tính năng IDS ?
    a. Network sniffer
    b. N-IDS (Network-based IDS)
    c. H-IDS (Host-based IDS)
    d. VPN
39. Acknowledgement, Sequencing, and Flow control là đặc tính của lớp nào trong mô hình OSI?
    a. Layer 2
    b. Layer 3
    c. Layer 4
    d. Layer 5

40. Giao thức nào trong các lớp mạng của mô hình tham chiếu OSI chịu trách nhiệm xác định đường dẫn và chuyển mạch?
    a. LAN
    b. Routing
    c. WAN
    d. Network
41. Data Encryption Standard là một ví dụ của :
    a. mã hóa công khai RSA
    b. mã hóa bằng phần cứng
    c. mã hóa đối xứng
    d. mã hóa không đối xứng
42. Khi một hacker cố gắng để tấn công một máy chủ thông qua Internet nó được gọi là loại tấn công?
    a. Physical access
    b. Remote attack
    c. Local access
    d. Internal attack
43. Điều nào sau đây là một công cụ để thực hiện footprinting không bị phát hiện?
    a. Traceroute
    b. Ping sweep
    c. Whois search
    d. Host scanning
44. Điểm yếu nào sau đây là chủ yếu của môi trường mạng không dây
    a. Phần mềm giải mã (Decryption software)
    b. IP spoofing (Giả mạo IP)
    c. A gap in the WAP (Một khe hở trong WAP)
    d. Định vị nơi làm việc (Site survey)
45. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì??
    a. Enumeration
    b. System hacking
    c. Active information gathering
    d. Scanning
46. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hoá dữ liệu?
    a. DSA
    b. ECC
    c. 3DES
    d. AES
47. Điều nào sau đây không phải là mục tiêu thiết kế bảo mật vật lý
    a. Ăn cắp dữ liệu bí mật
    b. Hack hệ thống từ bên trong
    c. Hack hệ thống từ Internet
    d. truy cập vật lý

48. Văn bản sau khi được mã hóa, được gọi là gì ?
    a. Chứng chỉ
    b. Mật mã đối xứng
    c. Khóa công khai
    d. Văn bản mã
49. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên (session) của mô hình OSI
    a. Circuit level firewall
    b. Packet filtering firewall
    c. Application level firewall
    d. Stateful multilayer inspection firewall
50. Loại Firewall nào sau đây cho phép hoạt động ở lớp mạng (network) của mô hình OSI
    a. Circuit level firewall
    b. Packet filtering firewall
    c. Application level firewall
    d. Stateful multilayer inspection firewall
51. Loại Firewall nào sau đây cho phép hoạt động ở lớp ứng dụng (application) của mô hình OSI
    a. Circuit level firewall
    b. Packet filtering firewall
    c. Application level firewall
    d. Stateful multilayer inspection firewall
52. Công cụ nào dưới đây có thể bị hacker sử dụng để tấn công Man In The Middle ?
    a. WireShark
    b. Ettercap
    c. Nmap
    d. Windump
53. Enumeration sẽ không phát hiện được những thông tin gì dưới đây?
    a. Services
    b. User accounts
    c. Ports
    d. Shares
54. Một phương pháp sử dụng công nghệ thấp thu thập thông tin cho các cuộc tấn công mạng trong tương lai là gì?
    a. Social engineering
    b. Man-in-the-middle
    c. Back doors
    d. Masquerade
55. Các phương pháp sinh trắc học nào sau đây được coi là an toàn nhất ?
    a. Phân tích chữ ký
    b. Quét tiếng nói

c. Lấy dấu bàn tay
d. Không quan trọng

56. Xử lý dữ liệu (data manipulation) là một cuộc tấn công ?
a. Confidentiality
b. Integrity
c. Authentication
d. Access

57. Điều gì sẽ không được coi là một phần của chính sách bảo mật?
a. Remote access
b. Employee comfort
c. Access control
d. Password length

58. Phương pháp lập bản đồ một mạng lưới gọi là gì?
a. Nghe trộm (Eavesdropping)
b. Do thám (Reconnaissance)
c. Sniffing
d. Khám phá (Discovery)

59. Thiết bị nào sử dụng bộ lọc gói và các quy tắc truy cập để kiểm soát truy cập đến các mạng riêng từ các mạng công cộng , như là Internet ?
a. Điểm truy cập không dây
b. Router
c. Tường lửa
d. Switch

60. Tường lửa loại Packet Filter được đặt tại lớp:
a. Physical
b. Data link
c. Network
d. Transport

61. Điều nào sau đây có thể được sử dụng để xác định tường lửa?
a. Search engines
b. Email
c. Port scanning
d. Google hacking

62. Thuật giải MD5 cho ta một giá trị băm có độ dài :
a. 156 bit
b. 256 bit
c. 128 bit
d. 512 bit

63. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như là web, FTP, và các máy chủ email ?
a. VPN
b. DMZ
c. VLAN

d. Intranet

64. Thiết bị nào cho phép ta kết nối đến một mạng LAN của công ty qua Internet thông qua một kênh được mã hóa an toàn ?
    a. VPN
    b. WEP
    c. Modem
    d. Telnet
65. Hệ thống nào sau đây được thiết kế để thu hút và xác định tin tặc?
    a. Firewall
    b. honeypot
    c. Honeytrap
    d. IDS
66. Một hệ thống mà thực hiện việc nhận dạng tấn công và cảnh báo cho một mạng gọi là gì?
    a. HIDS
    b. NIDS
    c. Anomaly detection HIDS
    d. Signature-based NIDS
67. Câu lệnh command line nào thực hiện chạy snort
    a. snort –l c:\snort\log –c C:\snort\etc\snoft.conf –A console
    b. snort –c C:\snort\etc\snoft.conf –A console
    c. snort –c C:\snort\etc\snoft.conf console
    d. snort –l c:\snort\log –c –A
68. Snort gọi là chương trình gì?
    a. NIDS
    b. Sniffer and HIDS
    c. Sniffer, HIDS, and traffic-logging tool
    d. NIDS and sniffer
69. Có hai component cần thiết trong quá trình cài đặt Snort là gì? (chọn 2)
    a. Snort rules
    b. Snort signatures
    c. Snort Engine
    d. Snort processor
70. Chức năng nào của IDS đánh giá dữ liệu được thu thập từ các cảm biến?
    a. Operator
    b. Manager
    c. Alert
    d. Analyzer
71. Kiểu phần mềm nào có thể sử dụng để ngăn chặn, phát hiện các hành động phá hoại trên một hệ thống?
    a. Personal Firewall
    b. IDS – host based

c. Antivirus
d. Tất cả các phương án trên

72. Kỹ thuật nào được sử dụng để bảo đảm thông tin liên lạc qua một mạng không được bảo mật ?
a. Telnet
b. SLIP
c. VPN
d. PPP

73. PGP (Pretty Good Privacy) cung cấp các chức năng nào sau đây?
a. Confidentiality
b. Integrity
c. Authenticity
d. Tất cả các chức năng trên.

74. Một khóa yếu (weak key) của một thuật toán mật mã có đặc tính nào sau đây?
a. Nó quá ngắn vì vậy dễ dàng bị phá vỡ
b. Nó chỉ có thể sử dụng như một khóa công khai
c. Nó có nhiều số không hơn số một
d. Nó tạo điều kiện dễ dàng trong việc tấn công thuật toán

75. Biện pháp nào sau đây được dùng để đảm bảo an ninh cho mạng Wi-fi
a. WEB
b. HTTPS
c. WPA2/WPA3
d. SSL

76. Sự khác nhau cơ bản giữa hai thuật toán MD5 và SHA là gì?
a. Sự an toàn - MD5 có thể bị giả mạo còn SHA thì không.
b. SHA có giá trị đầu ra 160 bit còn MD5 có giá trị đầu ra 128 bit
c. MD5 có giá trị đầu ra 160 bit còn SHA có giá trị đầu ra 128 bit
d. Sự an toàn - SHA có thể bị giả mạo còn MD5 thì không.

77. --------- là một tấn công ---------- cho phép nghe trộm trên đường truyền (chọn 2)?
a. Passive
b. Active
c. Wiretapping
d. Password cracking

78. Phương pháp nào sau đây có ưu điểm về khả năng sử dụng các mật khẩu mạnh, quản trị mật khẩu dễ dàng, và truy nhập tài nguyên nhanh?
a. Smartcards
b. PKI
c. Single Sign-on (SSO)
d. Kerberos

79. IKE (Internet Key Exchange) được sử dụng kết hợp với giao thức nào sau đây?
a. IPSec

b. SSL
c. Kerberos
d. Tất cả các giao thức trên

80. PDIOO tương ứng với lựa chọn nào sau đây?

a. Purpose, design, install, operation, optimization
b. Plan, design, install, operation, optimization
c. Plan, design, implement, operate, optimize
d. Purpose, design, implement, operate, optimize

81. Gửi một gói tin ICMP có kích thước lớn hơn 64Kb là một ví dụ của kiểu tấn công nào sau đây?

a. Buffer Overflow
b. Ping of Death
c. Syn Flooding
d. Tear Drop

82. Phần nào là quan trọng nhất trong phần mềm diệt virus?

a. Desktop
b. Definitions
c. Engine
d. Heuristics

83. Mô hình tham chiếu nào dưới đây mô tả các giao thức và dịch vụ truyền thông của máy tính trên mạng?

a. IETF – Internet Engineering Task Force
b. ISO – International Standards Organization
c. IANA – Internet Assigned Numbers Authority
d. OSI – Open System Interconnection

84. Giao thức IPSEC được sử dụng ở tầng nào trong mô hình OSI?

a. Layer 6 – Presentation
b. Layer 5 – Session
c. Layer 4 – Transport
d. Layer 3 – Network

85. Virus boot sector được kích hoạt khi nào trong các sự kiện sau?

a. Khởi động lại máy tính
b. Xóa file
c. Ghi file
d. Vào ngày 16 tháng 3.

86. Sự khác nhau cơ bản giữa logic bomb và stealth virus?

A. Các Stealth virus đưa ra các AV engine với thông tin sai để ngăn chặn phát hiện

B. Stealth virus thường trú trên bộ nhớ trong khi logic bomb ghi trên ổ đĩa.
C. Stealth virus
D. Logic Bomb

87. Phần nào sau đây là phần nguy hiểm nhất trong một chương trình virus?
a. Code
b. Payload
c. Strain
d. Không có phần nào nêu trên

88. MD5 là một thuật toán ……..
a. Hàm băm
b. 3DES
c. 192 bit
d. PKI

89. Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là?
a. Syn Flood
b. Ping of Death
c. Buffer Overflow
d. Password

90. Hệ thống kiểm soát truy cập giữa các vùng mạng
a. Router
b. Switch Layer 3
c. Firewall
d. Modem

91. Hệ thống IDS phát hiện dấu hiệu tấn công dựa vào
a. IP nguồn được định nghĩa trước
b. IP đích được định nghĩa trước
c. Signature
d. IP nguồn và IP đích

92. Cơ quan bạn có thêm một chi nhánh mới, để kết nối chi nhánh mới vào mạng trung tâm với chi phí hợp lý và đảm bảo an toàn, bạn sử dụng công nghệ nào ?
a. Leased line
b. Frame Relay
c. VPN qua ADSL
d. HDSL

93. Hình thức tấn công nào sau đây không thể phát hiện bởi thiết bị IDS (*Intrusion Detection System*) ?
a. DoS (Denial of Service)
b. Khai thác các lỗ hổng phần mềm

c. Spoofed e- mail

d. Port scan

94. Dịch vụ nào sau đây là một dịch vụ đơn hay một máy phục vụ để lưu trữ, phân phối, và quản lý các khóa phiên mật mã ?

a. KDC

b. KEA

c. PKI

d. PKCS

95. Các cặp cổng – dịch vụ nào sau đây không đúng

a. HTTP:80

b. SSL:25

c. DNS:53

d. Telnet:23

e. POP3:110

96. Thuật toán AES công bố năm 2001 sử dụng khóa có độ dài:

a. 2048 bit

b. 1024 bit

c. 512 bit

d. 128 -256 bit

97. Trường có công dụng kiểm tra sự toàn vẹn của gói (IP, TCP, UDP, ICMP) là:

a. Flags

b. Time to Live

c. Checksum

d. Options

98. Hệ thống PKI ưu tín nhất thế giới hiện nay là

a. OpenCA

b. Microsoft

c. Geo Trust

d. VeriSign

99. Tường lửa không có tác dụng với

a. Bảo vệ các lớp bên trong

b. Cấm hoặc cho phép gói tin

c. Social Engineering

d. Kiểm soát luồng dữ liệu đi qua nó

100. Ứng dụng nào sau đây dùng để đính kèm Trojan với một tập tin khác

a. Insider

b. Fports

c. What’s running

d. One file exe maker

101. Có thể kiểm tra các ports đang mở với:

a. Msconfig
b. Tracert
c. Netstat
d. Ipconfig

102. Các nguyên tắc (rule) của firewall được xác định bởi:
a. Hành động
b. Giao thức
c. Điều kiện
d. Tên rule

103. SSH sử dụng cổng:
a. 22
b. 23
c. 24
d. 25

104. Kỹ thuật nào dưới đây không phải là kỹ thuật cơ bản của virus:
a. Thường trú
b. Lây nhiễm
c. Mã hóa
d. Đa hình

105. Việc sử dụng quân đội Zombie để tấn công trên mạng là hình thức tấn công:
a. Intrusion
b. Buffer Overflow
c. Repudiation
d. Ddos

106. Độ an toàn của hệ mật phụ thuộc vào
a. không gian khóa đủ lớn để phép vét cạn khóa là không thể thực hiện được
b. thuật toán, không gian khóa và bản mã
c. tính bí mật của thuật toán
d. hàm mã là hàm cửa sập một chiều

107. Điểm truy cập giả mạo là gì?
a. Một điểm truy cập không được quản lý bởi một công ty
b. Điểm truy cập không được quản lý
c. Điểm truy cập thứ hai
d. Một thiết bị honeypot

108. Social engineering được thiết kế để_____:
a. Sửa đổi hành vi con người
b. Làm cho mọi người không tin tưởng
c. Lây nhiễm một hệ thống

d. Đạt được lợi thế về vật lý

109. What provides for both authentication and confidentiality in IPSec?
a. AH
b. IKE
c. OAKLEY
d. ESP

110. Giao thức IPSec thực hiện ở lớp nào?
a. Application
b. Transport
c. Network
d. Data-link

111. Có thể kiểm tra các port đang mở với:
a. Msconfig
b. Tracert
c. Wireshark
d. Netstat

112. Có khả năng lan truyền như chương trình độc lập mà không cần lan truyền qua tập tin:
a. Zombie
b. Virus
c. Spyware
d. Worm

113. Thuật toán chia Euclid mở rộng dùng để
a. tính nhanh một lũy thừa với số lớn
b. tính phần tử nghịch đảo của phép nhân
c. kiểm tra nhanh một số nguyên tố lớn
d. tính phần tử nghịch đảo của phép nhân và tìm ước chung lớn nhất

114. MAC là một từ cấu tạo bằng những chữ đầu của một nhóm nào liên quan đến mật mã?
a. Kiểm soát truy cập phương tiện (Media access control)
b. Kiểm soát truy cập bắt buộc (Mandatory access control)
c. Mã xác thực thông điệp (Message authentication code)
d. Các ủy ban đa tư vấn (Multiple advisory committees)

115. Công nghệ và quy trình được thiết kế để bảo vệ mạng và thiết bị khỏi bị tấn công, hư hỏng hoặc truy cập trái phép
a. An ninh mạng (Cyber Security)
b. Hacker mũ trắng (White Hat Hacker)
c. Máy chủ tên miền (Domain Name Server)
d. Tất cả câu trên đều đúng

116. Điều nào trong số này là dấu hiệu cho thấy trang web này an toàn.

a. http;//
b. http://
c. https:\\
d. https://

117. là các chương trình hoặc quy trình cho phép tin tặc duy trì quyền kiểm soát hệ thống máy tính.?
a. Antivirus
b. worms
c. exploits
d. firewall

118. Việc xâm phạm thông tin bí mật thuộc loại nào?
a. Bug
b. Vulnerability
c. Attack
d. Threat

119. Xác định phần mềm độc hại không sao chép hoặc sao chép thông qua lây nhiễm?
a. Trojans
b. Worms
c. Rootkits
d. Virus

120. Công cụ nào sau đây được sử dụng để hack Wi-fi?
a. Wireshark
b. Norton
c. Cloud scan
d. Aircrack-ng

121. Mạng riêng ảo, hay VPN, là kết nối _____ qua Internet.
a. Giải mã
b. Mã hóa
c. Có dây
d. Không dây

122. Những lý do để sử dụng VPN là gì?
a. Quá trình tương tác với người khác để trao đổi thông tin và phát triển các mối quan hệ chuyên môn hoặc xã hội.
b. Quá trình chuyển đổi văn bản mã hóa thành văn bản thuần túy
c. Quá trình chuyển đổi thông tin hoặc dữ liệu thành mã, đặc biệt là để ngăn chặn truy cập trái phép
d. Quá trình xử lý các thuộc tính và thao tác của các con số.

123. Những lý do để sử dụng VPN là gì?
a. Ngăn chặn người dùng trái phép theo dõi lưu lượng truy cập của bạn

b. Ngăn chặn người dùng được phép theo dõi lưu lượng truy cập của bạn
c. Cho phép người dùng thực hiện công việc từ một vị trí
d. Cho phép người dùng thực hiện công việc từ xa.

124. Tìm kiếm các mẫu mạng cụ thể do phần mềm độc hại đã biết tạo ra.
a. Dựa trên chữ ký
b. Hệ thống phát hiện xâm nhập máy chủ (HIDS)
c. Dựa trên bất thường
d. Chức năng bảo mật

125. Bao gồm cảm biến và bảng điều khiển
a. Network-based IDS (NIDS)
b. Host-based IDS (HIDS)
c. Protocol IDS (PIDS)
d. Distributed IDS (DIDS)

126. Bao gồm các agents (đại diện) và bảng điều khiển
a. Network-based IDS (NIDS)
b. **Host-based IDS (HIDS)**
c. Protocol IDS (PIDS)
d. Distributed IDS (DIDS)

127. Tiêu chuẩn an toàn thông tin Việt Nam năm 2015 có bao nhiêu nhóm?
a. 10
b. 11
c. 12
d. 13

128. Tiêu chuẩn an toàn thông tin ISO/IEC 17799 có bao nhiêu nhóm?
a. 10
b. 11
c. 12
d. 13

129. Khái niệm nào sau đây được sử dụng để mô tả sự không thể chối từ của người gửi khi gửi thông điệp?
a. Toàn vẹn
b. Tính không chối từ (non-repudiation)
c. Xác thực
d. Tính tin cậy

130. Thuật giải Difie Hellman dùng để:
a. Bảo mật thông điệp
b. Xác thực thông điệp
c. Phân phối khoá trước cho hệ mật đối xứng
d. Lấy chữ ký số

131. Các loại khoá mật mã nào sau đây dễ bị crack nhất?

a. 128 bit
b. 256 bit
c. 40 bit
d. 56 bit

132. Trọng tâm chính của kế hoạch phục hồi sau thảm họa là gì?
a. Giảm chi phí công ty
b. Nhanh chóng đưa hoạt động kinh doanh trở lại bình thường
c. Tuyển dụng nhân viên mới
d. Nâng cao chiến lược tiếp thị

133. Mục đích của chính sách bảo mật là gì?
a. Thực thi quy định về trang phục
b. Điều chỉnh hành vi của người dùng và xác định phản ứng đối với các sự cố
c. Đặt mục tiêu doanh thu của công ty
d. Xác định chiến lược tiếp thị

134. Tuổi mật khẩu tối đa được khuyến nghị trong tài liệu là bao nhiêu?
a. 110-120 ngày
b. 20 ngày
c. **60-90 ngày**
d. 30 ngày

135. Xác thực đa yếu tố (MFA) yêu cầu những gì?
a. Chỉ cần một mật khẩu
b. **Hai hoặc nhiều yếu tố xác minh**
c. Một lần quét sinh trắc học
d. Một tên người dùng duy nhất

136. Phương pháp mã hóa nào sử dụng một khóa duy nhất cho cả mã hóa và giải mã?
a. **Mã hóa đối xứng**
b. Mã hóa bất đối xứng
c. Băm
d. Mã hóa khóa công khai

137. Lợi ích nào sau đây là lợi ích của việc áp dụng quyền tập tin và thư mục phù hợp?
a. Giảm chi phí phần cứng
b. Nâng cao hiệu suất phần mềm
c. **Ngăn chặn truy cập trái phép**