ÔN TẬP ATTT - sss

Hệ Thống Thông Tin Quản Lý (Trường Đại học Kinh tế, Đại học Đà Nẵng)

TRẮC NGHIỆM ATBMTT

1. **Hành vi ảnh hưởng đến tính khả dụng của hệ thống thông tin**

a. Sao chép tài liệu của một người khác
b. Viris xoá mất các tập tin trên đĩa cứng.
c. Mất điện thường xuyên làm hệ thống máy tính làm việc gián đoạn
d. Tất cả các hành vi trên.

2. **Chọn câu đúng**

a. Có thể ngăn chặn các tấn công tràn bộ đệm bằng các phần mềm antivirus
b. Có thể ngăn chặn các tấn công tràn bộ đệm bằng cách cài đặt firewall
c. Tất cả các phần mềm viết bằng ngôn ngữ C đề có chứa lỗi tràn bộ đệm
d. Lỗi tràn bộ đệm chỉ xáy ra trên các phần mềm có nhập dữ liệu từ người dùng

3. **Để xác định máy đích có cổng dịch vụ nào ta sử dụng kỹ thuật**

a. Network scanning
b. Port scanning
c. Vulnerability scanning
d. Tất cả đều đúng

4. **Kỹ thuật tấn công sử dụng ICMP và MTU để làm sụp hệ thống được gọi là tấn công**

a. Man in the middle
b. Giả mạo
c. Ping of death
d. SYN flood

5. **Đặc trưng của các Trojan là?**

a. Chỉ hoạt động trên hệ điều hành DOS
b. Không có khả năng tự lây lan
c. Tự động phát tán qua email
d. Tự động phát tán qua lỗ hổng phần mềm.

6. **Biện pháp nào sau đây được sử dụng trong Wifi để kiểm soát việc truy cập theo từng card mạng?**

a. WEP
b. MAC Filtering
c. WPA
d. Bỏ broadcast SSID

7. **Một thông điệp như sau được gửi đi "ABC" bên nhận nhận được thông điệp có nội dung là "ABC123",quá trình truyền thông tin đã can thiệp ở giữa. tính chất nào sau đây đã bị ảnh hưởng sau quá trình truyền tin này.**

a. Tính bí mật

b. Tính sẵn sàng
c. Tính toàn vẹn
d. Tính bí mật và tính toàn vẹn

8. Một nhà quản trị mạng mới thay thế Hub bằng Switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa máy khác trong mạng với máy chủ. Giả sử thiết bị Switch hoạt động tốt, khả năng xảy ra là;

a. Trừ thông tin Broadcast, switch không gửi thông tin ra tất cả các cổng
b. Switch được cấu hình VLAN
c. Phần mềm Sniffer cấu hình sai
d. Phần mềm Sniffer không bắt được thông tin qua công Ethernet.

9. "Internal Zone" là:

a. Vùng tin cậy và là nơi bố trí các máy tính và thiết bị làm việc của Users
b. Vùng phi quân sự dủng để đặt những dịch vụ để public ra Internet
c. Vùng không tin cậy, vùng này là Internet
d. A,B,C đều sai.

10. Tường lửa là thiết bị dùng để

a. Phát hiện và diệt virus
b. Quản trị mạng
c. Theo dõi luồng thông tin đi qua nó
d. A,B,C đều sai.

11. 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 Internet

a. Điểm truy cập không dây
b. Router
c. Tường lửa
d. Switch

12. Người dùng đặt mật khẩu của họ sử dụng những từ đơn giản và dễ đoán như tên một con vật, ngày sinh,… có thể sử dụng kiểu tấn công nào sau đây

a. Tấn công kiểu từ điển
b. Tấn công Brute Force
c. Tấn công giả mạo
d. Tấn công MITM (Man in the midle)

13. Giao thức nào sau đây được dùng để bảo mật mạng wifi

a. WEB
b. HTTPS

c. WPA 2
d. SSL

14. Phân vùng DMZ

a. Được sử dụng nhằm nâng cao tính an ninh, an toàn, bảo mật những vị trí trọng yếu trong toàn bộ hệ thống mạng
b. Là vùng đệm tập trung hệ thống phân luồng, kiểm soát gói tin, cung cấp dịch vụ cho bên trong và bên ngoài hệ thống
c. Toàn bộ thông tin từ bên ngoài vào bên trong hoặc ngược lại đều phải đi qua DMZ và chịu sự quản lý, điềukhiển của phân vùng này
d. Tất cả đều đúng

15. Chức năng của hệ thống honeypot là

a. Giả lập các hệ thống/dịch vụ thật để đánh lừa Hacker
b. Tấn công vào hệ thống của Hacker
c. Ngăn chặn tấn công của Hacker
d. Phát hiện và ngăn chặn tấn công của Hacker

16. Công cụ nào cho phép theo dõi các kết nối trong thời gian thực

a. Netstat
b. Fport
c. TcpView
d. Ettercap

17. Virus máy tính là gì?

a. phần mềm do lỗ hổng của website tạo ra
b. phần mềm do lỗ hỏng của windows tạo ra
c. phần mềm do con người viết ra nhằm mục đích phá hoại
d. phần mềm được tại ra ngoài ý muốn do lỗi lập trình của người viết

18. bảo mật thông tin là đảm bảo

a. tính bảo mật
b. tính toàn vẹn
c. tính sẵn sàng
d. tất cả đều đúng

19. nguyên tắc xây dựng một hệ thống bảo mật

a. áp dụng các cơ chế an toàn phù hợp với hệ thống
b. xây dựng các chính sách an toàn chặt chẽ
c. xây dựng chính sách bảo mật và triển khai các cơ chế để đảm bảo chính sách đó
d. tất cả đều đúng

20. để bẻ khoá mật khẩu bắt được, có thể sử dụng công cụ nào sau

a. wireshark

b. secureCRT
c. Cain&Abel
d. Havij

21. Kiểu xác thực được dùng phổ biến

a. Certificate
b. Token
c. Mật khẩu
d. Sinh trắc học

22. Một máy chủ trên mạng không chấp nhận các kết nối TCP và thông báo rằng nó đã vượt quá giới hạn của phiên làm việc. có thể xảy ra cuộc tấn công.

a. Tấn công TCP ACK (Tấn công kiểu SYN/ACK)
b. Tấn công smurf
c. Tấn công virus
d. TCP/IP hijacking

23. Kỹ thuật tấn công nào sau đây không dựa trên giao thức TCP/IP

a. SYN/ACK flooding
b. TCP sequence number attack
c. ICMP attack
d. Software exploitation

24. Cơ chế bảo vệ hệ thống Simple packet Filter không có khả năng làm được việc nào sau:

a. Quét virus
b. Lọc gói tin theo IP
c. Lọc gói tin theo Port
d. Lọc gói tin theo giao thức

25. Để bắt gói tin trên mạng, có thể sử dụng công cụ nào sau

a. Wireshark
b. SecureCRT
c. Cain&abel
d. Havij

26. Một website tồn tại lỗ hỏng SQL Injection nguy cơ cao nhất có thể xảy ra là

a. Tấn công thay đổi hình ảnh giao diện
b. Xoá toàn bộ cơ sở dữ liệu
c. Mất username/password của quản trị
d. Máy chủ bị chiếm quyền điều khiển

27. Hệ thống kiểm soát truy cập giữa các vùng mạng

a. Router

b. Switch layer 3
c. Firewall
d. Modem

28. Câu lệnh: union select 1,group_concat(column_name),3,4,5,6 from information_scheme.columns where table_name=char(97,100,109,105,110) dùng để truy cấn trên table.

a. Admin
b. User
c. Sinhvien
d. Table

29. Kỹ thuật tấn công nào sau đây liên quan đến giao dịch IP

a. Mã nguồn độc hại
b. Giả mạo IP
c. Tấn công dạng Man in the midle
d. Tấn công chuyển tiếp

30. Chương trình sniffer thực hiện bắt các gói tin ở tầng nào sau:

a. Tầng Transport, Network
b. Tầng Network, Datalink, Physical
c. Tầng Transport, Presentationm Session
d. Tấng Session, Transport, Network

31. ứng dụng của giao thức bảo mật IPSec

a. xây dựng các website an toàn cho các ứng dụng thương mại điện tử
b. xây dựng các trang mang riêng ảo VPN trên nền mạng Internet công cộng
c. cho phép truy xuất từ xa một cách an toàn
d. tất cả các ứng dụng trên

32. kỹ thuật khai thác phiên kết nối giữa các máy tính là kỹ thuật tấn công nào sau đây

a. SQL Injection
b. Dos
c. Sesion Hijacking
d. System Hacking

33. Quyền truy cập nào cho phép ta hiệu chỉnh thuộc tính của một tập tin

a. Hiệu chỉnh
b. Sao chép
c. Thay đổi
d. Biên tập

34. Để tấn công nhiễm độc gói tin trên mạng, có thể sử dụng công cụ nào sau

a. Wireshark
b. secureCRT
c. cain&abel
d. havij

35. Loại tấn công nào sau đây khi thực hiện đồng thời trên nhiều máy

a. DoS
b. DosS
c. Back door
d. Social engineering

36. Công cụ nào sau đây có thể dùng để bắt mật khẩu của người dùng trong mạng

a. Cain&abel
b. Wireshark
c. Tcpdump
d. Ettercap

37. Các cơ chế đảm bảo tính toàn vẹn của thông tin

a. Gồm các cơ chế ngăn chặn và cơ chế phát hiện các vi phạm về toàn vẹn thông tin
b. Mật mã hoá toàn bộ thông tin trong hệ thống
c. Lưu toàn bộ thông tin trong hệ thống dưới dạng nén
d. Tất cả các cơ chế trên

38. Hình thức tấn công nào sau không phải là tấn công chủ động

a. Tấn công nghe lén
b. Tấn công từ chối dịch vụ
c. Tấn công replay
d. Tấn công giả mạo

39. Mục tiêu chủ yếu của kiểu tấn công Social Engineering nhằm vào:

a. Email
b. Local area network
c. Con người
d. Peer to peer network

40. Hacker phát tán virus và điều khiển các máy tính bị nhiễm virus tấn công một hệ thống máy chủ. Đây là kiểu tấn công

a. Tấn công sử dụng Flash
b. Tấn công sử dụng Botnat
c. Tấn công sử dụng SYN FLOOD
d. Tấn công sử dụng Replay của DNS server

41. Quá trình thu thập thông tin trên máy đích được gọi là

a. DoS
b. SQL Injection
c. Scannning
d. footPrinting

42. phương thức tấn công nào ngăn chặn các user hợp lệ truy xuất các tài nguyên hệ thống
a. sniffing
b. spoofing
c. DoS
d. Man in the midle

43. Phần mềm có chức năng ngăn chặn hành vi cho phép
a. Theo dõi các hành vi trong thời gian thực của hệ thống
b. Phát hiện code có hại trước khi chúng thực hiện
c. Theo dõi các tham số của hệ thống
d. Tất cả đều đúng

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

45. Công cụ nào dưới đây có thể bị hacker sử dụng để tán công MITM
a. Wireshark
b. Ettercap
c. Nmap
d. Windump

46. Để phát hiện máy tính có đang bị tấn công, điều khiển từ xa không người ta có thể dùng những cách nào
a. Kiểm tra kết nối trên máy tính
b. Quét cổng
c. Phân tích dữ liệu mạng
d. Cả 3 đáp án

47. Local attack là kiểu tấn công
a. Từ một website kiểm soát các website khác trên máy chủ
b. Tấn công trong mạng nội bộ
c. Man in the midle trong LAN
d. APR Spoofing

48. Chức năng của mật mã thông tin là

a. Bảo vệ tính toàn vẹn thông tin
b. Bảo vệ tính bí mật thông tin
c. Bảo vệ tính khả dụng của thông tin
d. Bảo vệ tính không thể phủ nhận của thông tin

49. Tiêu chuẩn về quản lý thông tin là
a. ISO 17799:2005
b. ISO 27001:2005
c. ISO 27001:2013
d. ISO9001:2005
e. TCVN 7562:2005

50. Hình thức tấn công nào sau xảy ra khi một chuỗi dữ liệu được gửi tới một vùng đệm mà có kích thước lớn hơn khả năng được thiết kế ra của vùng đệm
a. Tấn công Brute Force
b. Buffer overflow
c. Tấn công Man in the midle
d. Syn Flood

51. Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm hệ điều hành
a. Cài đặt bản service pack mới nhất
b. Cài đặt lại hệ điều hành thông dụng
c. Sao lưu hệ thống thường xuyên
d. Shutdown hệ thống khi không sử dụng

52. Nguyên tắc hoạt động của một hệ thống IDS
a. Phân tích các gói dữ liệu lưu trong trên mạng để tìm dấu hiệu của tấn công
b. Phân tích các dữ liệu trong nhật ký hệ thống để phát hiện dấu hiệu tấn công
c. Duy trì một cơ sở dữ liệu về các dấu hiệu tấn công
d. Tất cả các điều trên

53. Nguyên tắc đảm bảo an toàn cho mật khẩu đối với người sử dụng
a. Quy định thời gian sử dụng tối đa của mật khẩu
b. Không dùng mật khẩu quá ngắn, mật khẩu có chứa tên người dùng, mật khẩu là những từ có nghĩa trong từ điển
c. Mã hoá mật khẩu khi lưu trữ
d. Tất cả đều đúng

54. Điều gì xảy ra khi máy X sử dụng kỹ thuật ARP Spoofing để nghe lén thông tin từ máy Y
a. X giả mạo địa chỉ MAC của Y
b. X giả mạo địa chỉ IP của Y

c. Y giả mạo địa chỉ MAC của X
d. Y giả mạo địa chỉ IP của X
55. Chức năng của Firewall
a. Firewall chỉ có thể ngăn chặn các tấn công từ bên ngoài hệ thống
b. Tất cả các gói dữ liệu đi qua firewall đều bị đọc toàn bộ nội dung, nhờ đó firewall mới có cơ sở để phân biệt các tấn công với các loại lưu lượng khác
c. Nếu mở tất cả các cổng trên firewall thì firewall sẽ hoàn toàn bị vô hiệu hoá
d. Tất cả đều đúng
56. Chức năng của cơ chế kiểm tra trên hệ thống
a. Ghi lại, phân tích, thông báo
b. Theo dõi và ghi nhận các sự kiện và hành vi diễn ra trên hệ thống
c. Cung cấp thông tin để phục hồi hệ thống khi có sự cố
d. Cung cấp thông tin làm chứng cứ cho các hành vi vi phạm chính sách an toàn hệ thống
57. Loại firewall nào sau đây có khả năng xác thực người sử dụng
a. Simple packet filter
b. Stateful packet filter
c. Application level
d. Tất cả đều sai
58. Kỹ thuật chèn vào các website động những đoạn mã script nguy hiểm là tấn công
a. XSS
b. CSS
c. SQL Injection
d. DoS
59. ứng dụng nào sau đây có chức năng thay đổi địa chỉ IP của tất cả các gói dữ liệu đi qua nó
a. IDS
b. Proxxy
c. NAT
d. Không có ứng dụng nào sau đây
60. Email server nên được đặt ở vùng mạng nào
a. Inside zone
b. Outside zone
c. Demillitaeized zone
61. Lỗ hổng 0-day không phải là
a. Lỗ hổng nhà sản xuất chưa kịp vá
b. Lỗ hỏng phá hoại hệ thống trong vòng 1 ngày

c. Lỗ hổng hacker chưa công bố rộng rãi
d. Lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ
62. Firewall hoạt động ở những lớp nào của mô hình OSI
a. Layer 2, layer 3, layer 4, layer 7
b. Layer3, layer 4, layer 7
c. Layer 2, layer 4, layer7
d. Layer 3, layer 4, layer 5, layer 7
63. Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên may tính
a. Netsata
b. Ipconfig
c. Ping
d. Tracert
64. Chức năng của Authentication dùng để làm gì
a. Dùng để xác thực người dùng khi đăng nhập vào hệ thống
b. Dùng để phân quyền người dùng khi họ đăng nhập vào hệ thống thành công
c. Dùng để theo dõi người khi hoạt động trong hệ thống
d. Cả 3 đáp án đều sai
65. Nếu người A muốn ký một tài liệu và sau đó gửi đến một người khác, khoá nào phải được sử dụng
a. Khoá công khai của người A
b. Khoá công khai của bên nhận
c. Khoá cá nhân của bên nhận
d. Khoá cá nhân của người Ayg
66. Trong mật mã, khoá bí mật dùng để làm gì
a. Mã hoá và ký
b. Giải mã và kiểm tra chữ ký
c. Giải mã và ký
d. Kiểm tra chữ ký
67. Trong Blockchain, P2P là viết tắt của gì?
a. Password to password c
b. Peer to peer
c. Product to product
d. Private key to public key
68. Chứng nhận điện tử được sử dụng để làm gì
a. Mã hoá dữ liệu
b. Giải mã dữ liệu

c. Chứng minh người sở hữu khoá công khai
d. Hash
69. Mục đích của tấn công DoS là
a. Phá hoại Database
b. Tấn công để làm giảm khả năng cung cấp dịch vụ của server
c. Thu thập thông tin của đối tượng tấn công
d. Cả 3 đáp án đều sai
70. Thế nào là tính bảo mật của hệ thống thông tin
a. Là đặc tính của hệ thống trong đó thông tin được giữ bí mật không cho ai truy xuất
b. Là đặc tính của hệ thống trong đó tất cả thông tin được lưu trữ dưới dạng mật mã
c. Là đặc tính của hệ thống trong đó chỉ có những người dùng được cho phépmowis có thể truy xuất được thông tin
d. Tất cả đều đúng
71. A muốn mã hoá thông điệp M trước khi gửi cho B và đảm bảo chỉ B mới có thể đọc được thì A sẽ dùng khoá
a. Khoá công khai của B: PUB
b. Khoá riêng của B: PRB
c. Khoá công khai của A: PUA
d. Khoá riêng của A: PRA
72. Trong Blockchain, tiền kỹ thuật số được lưu trữ ở đâu
a. Tài khoản ngân hàng
b. Dĩa mềm
c. Ví điện tử
d. Trong túi bạn
73. ứng dụng của mã hoá bất đối xứng
a. bảo mật thông tin
b. xác thực thông tin
c. bảo vệ tính khả dụng của hệ thống
d. câu a và b
74. các loại khoá mật mã nào sau đây dễ bị tấn công bẻ khoá nhất
a. 128 bit
b. 40 bit
c. 256 bit
d. 56 bit
75. So sánh RSA và AES
a. RSA có tốc độ thực thi bằng phần mềm cao hơn AES
b. RSA an toàn hơn AES

c. RSA dựa vào các hàm toán học còn AES dựa trên các thao tác xử lý bit
d. Bằng cách phân tích khoá công khai thì có thể tìm ra khoá bí mật của RSA, trong khi đó đối với cách duy nhất để tìm khoá là vét cạn

76. Mã hoá công khai RSA dựa trên cơ sở của bài toán nào sau
a. Phân tích các số lớn thành các thừa số nguyên tố
b. Tính logarithin rời rạc
c. Tính luỹ thừa và ghép toán module

77. Ai là người tạo ra bitcoin
a. Statoshi nakamoto
b. Sammsung
c. John mcafee
d. Apple

78. Các thuộc tính của một giải thuật chữ ký số
a. Phải xác nhận chính xác người ký và ngày giờ phát hành chữ ký
b. Phải xác thực nội dụng thông tin ngay tại thời điểm phát sinh chữ ký
c. Phải có khả năng cho phép kiểm chứng bởi một người thứ 3 để giải quyết khi có tranh chấp
d. Tất cả các câu trên

79. Trong blockchain, miner là gì
a. Một loại blockchain
b. Một thuật toán dự đoán chuỗi tiếp theo
c. Người tính toán để xác minh giao dịch
d. Máy tính xác nhận hợp lệ và xử lý giao dịch blockchain

80. Liệt kê các mục tiêu của an toàn hệ thống theo thứ tự ưu tiên giảm dần
a. Ngăn chặn, phát hiện, phục hồi
b. Phát hiện, ngăn chặn, phục hồi
c. Phát hiện và ngăn chặn
d. Phát hiện và phục hồi

81. Quá trình xác định vị trí và các thông tin của một máy trên mạng được gọi là
a. In dấu chân
b. Quét
c. Thiết bị làm nhiễu
d. Liệt kê

82. Blockchain là gì
a. Số cái phân phối tr zên mạng ngang hàng
b. Một loại tiền ảo
c. Một sàn giao dịch

d. Số cái tập trung

83. Tính toàn vẹn của hệ thống thông tin là đặc tính của hệ thống mà trong đó

a. Thông tin không bị sửa đổi hoặc xoá bỏ bởi người sử dụng

b. Thông tin không bị thay đổi theo thời gian

c. Thông tin không bị truy xuất bởi những người không được phép

d. Thông tin không bị thay đổi, hư hỏng hay mất mát

84. Máy chủ FTP của công ty ABC được cấu hình để truyền tpaj tin với độ tin cậy cao. Tuy nhiên, người sử dụng lại không thể kết nối đến máy chủ trên, trong khi họ vẫn kết nối được đến máy chủ web. Sau khi kiểm tra, người ta nhận thấy dịch vụ FTP đã được kích hoajtt. Cần phải làm gì để giải quyết sự cố

a. Kiểm tra các sự cho phép trên hệ thống tập tin NTFS đã được cấu hình đúng chưa

b. Kiểm tra các cổng 20. 21 đã được cho phép đi qua chưa trong bộ lọc TCP/IP

c. Kiểm tra cổng 80 đã được cho phép đi q ua chưa trong bộ lọc TCP/IP

d. Kiểm tra cổng 443 đã được cho phép đi qua chưa trong bộ lọc TCP/IP

85. Văn bản sau khi được mã hoá được gọi alf

a. Chứng chỉ

b. Mật mã đối xứng

c. Khoá công khai

d. Văn bản mã hoá

86. Để hạn chế khả năng bắt gói tin trong một mạng ta có thể

a. Sử dụng wifi

b. Sử dụng hub

c. Phân chia VLAN

d. Sử dụng tường lửa cá nhân

87. Chữ ký điện tử được dùng để

a. Xác nhận người dùng

b. Đảm bảo tính toàn vẹn

c. Mã hoá

d. A và b đúng

88. Dữ liệu đi kèm theo một thông điệp M nhằm mục đích xác nhận người chủ của thông điệp được gọi là

a. Secure mail

b. Blometric

c. Digital certificate

d. Digital signature

e. Đáp án khác

89. Một hệ thống gồm 10 thiết bị đầu cuối liên lạc với nhau sử dụng mật mã đối xứng, mỗi đầu cuối sử dụng các khoá bí mật khác nhau khi kết nối với mỗi thiết bị đấy cuối khác, có bao nhiêu khoá bí mật trên toàn hệ thống

a. 10 khoá
b. 20 khoá
c. 45 khoá
d. 90 khoá

90. Loại mã độc nào sau đây không có cơ chế tự động lây lan

a. Virus
b. Worm
c. Virus macro
d. Trojan

91. Kỹ thuật quét cổng NULL sử dụng các cờ TCP nào sau

a. ACK
b. SYN
c. FIN
d. RST
e. PSH
f. URG

92. Các nguy cơ của một hệ thống mật mã

a. Tấn công bằng cách dò khoá bí mật
b. Tấn công bằng phương pháp phân tích
c. Tấn công từ chối dịch vụ
d. Câu a và b

93. Giao thức nào được dùng để mã hoá dữ liệu trao đổi giữa web browser và web server

a. IPSec
b. HTTP
c. SSL
d. VPN

94. Thuật toán mã hoá AES sử dụng 12 vòng lặp có độ dài khoá là:

a. 192 bits
b. 64 bits
c. 128 bits
d. 256 bits

95. Trong mã hoá RSA cho khoá công khai(e,n)=(7,55), cho khoá bí mật (d,n)=(23,55). Cho văn bản mã hoá C=36. Văn bản gốc là 16

96. Chức năng của các hàm băm
a. Tạo ra một khối thông tin ngắn, cố định từ một khối thông tin gốc lớn hơn
b. Mật mã hoá thông tin
c. Xác thực nguồn gốc thông tin
d. Ngăn chặn việc phủ nhận hành vi chủ thể thông tin
97. Trong blockchain, Node là gì?
a. Một loại tiền ảo
b. Một chuỗi blockchain
c. Một máy tính trong mạng blockchain
d. Một sàn giao dịch
98. Giải thuật hàm băm nào có giá trị băm 16 bytes
a. MD5
b. SHA-1
c. DES
d. 3DES
99. Tấn công sniffer có thể được sử dụng để lấy thông tin về username và…
a. SSH
b. SSL
c. FTP
d. HTTPS
100. Trong mã hoá RSA cho khoá công khai (e,n)=97,55), khoá bí mật (23,55). Cho văn bản gốc P=4. Văn bản mã hoá C= 46
101. DES la 56 bit
102. Tat ca ket noi mang netstart
103. Giao thức SMTP sử dung cổng dịch vụ số 25
104. Giao thức POP3 sử dung cổng dịch vụ số110
105. Mail server thường sử dụng giao thức POP3 VÀ SMTP
106. HTTP sử dụng cổng dịch vụ số 80
107. HTTPS sử dụng cổng dịch vụ 443
108. A gởi gói tin có cờ SYN =1 giá trị segment khơi đầu có giá trị là SEQ(a)=0
109. B đồng ý kết nối SYN =1, ACK =1 thì giá trị SEQ(B)=0, ack (B)=1
110. Tcp đầy đủ TCP/SYN VÀ ACK ,RST

Quét Xmas : FIN , URG, PUSH
FIN : FIN và RST
NULL : Ack và RST
IDLE : TCP /IP và IDLIE , SYN , RST
UDP : ICMP

QUÉT ACK :Tường lửa , switch và Cam

111. **51% Attack** – Thuật ngữ này mô tả tình huống quá nhiều sức mạnh tính toán (hash power) của mạng lưới blockchain được tập trung tại một chỗ. Có thể một người hoặc một nhóm người dùng kiểm soát 51% sức mạnh tính toán, hệ thống có thể "bị" điều khiển một cách có chủ đích hoặc vô tình thực hiện các giao dịch xung đột xâm phạm đến hệ thống.
112. **Airdrop** – Token được phân phối miễn phí bởi một nhà phát triển mạng lưới Cryptocurrency.
113. **Altcoin** – Tất cả cryptocurrency ngoại trừ Bitcoin được gọi là Altcoin (viết tắt từ "alternative coin").
114. **ASIC** – Viết tắt của "Application Specific Integrated Circuit", ASIC là con chip được thiết kế đặc biệt. Trong thế giới của Blockchain, ASIC là con chip được phát triển để chạy phần mềm dùng trên các máy đào và được công nhận có khả năng vượt trội hơn CPU và GPU thông thường.
115. **Bitcoin** – Tiền điện tử đầu tiền và có tổng vốn hóa lớn nhất. Bitcoin được ra mắt vào năm 2009 dưới dạng tiền tệ phi tập chung (decentralized currency), được xây dựng trên công nghệ Blockchain.
116. **Blockchain** – Một cơ sở dữ liệu phi tập chung, được xây dựng trên một chuỗi các khối được liên kết với nhau. Tất cả các giao dịch trên mạng lưới được lưu trữ trên sổ kế toán (sổ cái) công khai, tồn tại trên toàn mạng, không cần một máy chủ trung tâm ủy quyền cho các giao dịch trên mạng.
117. Có thể bạn quan tâm: Phần mềm truy xuất nguồn gốc nông sản
118. **Cold Storage** – Biện pháp bảo mật lưu trữ cryptocurrency trong một môi trường ngoại tuyến (offline environment). Đây có thể là thiết bị lưu trữ (USB) hoặc ví giấy.
119. **Consensus** – Sự đồng thuận. Vì mạng lưới Blockchain mang tính phi tập chung (decentralized) nên sự đồng thuận là yếu tố vô cùng quan trọng.
120. **Cryptocurrency (Tiền mã hóa)** – Ứng dụng đầu tiên của Blockchain. Tiền mã hóa được thiết kế và lưu trữ trên mạng lưới phi tập chung với mỗi token và các giao dịch được mã hóa.
121. **DAO** – Viết tắt của "Decentralized Autonomous Organization". Một tổ chức được xây dựng dựa trên bộ quy tắc và quyền tự quyết có cấu trúc mô hình phân cấp của Blokchain, loại bỏ những thủ tục rườm rà và tốn kém chi phí về nhân lực.
122. **Dapps** – Viết tắt của "Decentralized apps". Về cơ bản, đây là những chương trình sử dụng Blockchain để tạo ra các ứng dụng chạy trên mạng phân cấp.
123. **Decentralized** – Mô hình phân tán phi tập chung, là mô hình mang ý tưởng chia phần việc ra và phân về cho những bộ phận nhỏ xử lý, ra quyết định ở cấp bộ phận. Quyền lực được chia đều đối lập hoàn toàn với mô hình Centralized.
124. **Digital signature** – Mã định danh duy nhất được cung cấp cho một người dùng, một token hoặc một giao dịch trong mạng lưới Blockchain.

125. **Distributed Ledger** – Công nghệ sổ cái phân tán là một mạng ngang hàng P2P (peer-to-peer) sử dụng các thuật toán đồng thuận, để đảm bảo việc sao lưu qua các node được thực hiện.

126. **Fork** – Sự thay đổi của một mạng lưới Blockchain, mỗi thay đổi phải được sự đồng thuận của người dùng. Nếu đủ số người dùng chấp nhận việc nâng cấp hoặc thay đổi mã code, Fork sẽ được triển khai trên toàn hệ thống. Một thay đổi mà vẫn hỗ trợ các phiên bản cũ của mạng, được gọi là Soft Fork. Một thay đổi không tương thích ngược lại, được gọi là Hard Fork. Đôi lúc, sự chia rẽ trong c

127. **Full Node** – Là một node thực thi đầy đủ các quy tắc của một mạng lưới Blockchain (chạy phần mềm đầy đủ của một mạng lưới Blockchain).

128. **Genesis block** – Khối (block) đầu tiên trên mạng Blockchain.

129. **Hash** – Một thuật toán sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu. Khi lưu trữ thông tin trên Blockchain, giá trị băm đóng vai trò là khóa cho việc xác định khối (block) bằng cách chuyển đổi thành một chuỗi các số và chữ cái.

130. **ICO** – Viết tắt của "Initial Coin Offering". Hình thức huy động vốn của các nhà đầu tư bằng các phát hành ra token từ nhà phát triển.

131. **Ledger** – Nhật ký kỹ thuật số của tất cả các giao dịch diễn ra trên mạng lưới Blockchain. Bản sao sổ kế toán được lưu trữ trên mạng và được cập nhật liên tục để phù hợp với nhau, vì vậy các giao dịch có thể được xác minh bởi bất kỳ ai kết nối với mạng.

132. **Lightning Network** – Một giải pháp được thiết kế để tăng tốc độ xử lý giao dịch trên mạng Blockchain. Mạng Lightning tạo ra một mạng P2P để xử lý các giao dịch, trước khi được ghi lại trên sổ cái công cộng Blockchain.

133. **Liquidity** – Thanh khoản. Có thể nhận ra, cryptocurrency dễ dàng chuyển đổi thành tiền mặt. Tính thanh khoản phụ thuộc vào nhiều yếu tố, bao gồm cả cung và cầu, thời gian xử lí giao dịch.

134. **Mining** – Hành động sử dụng sức mạnh máy tính để xác nhận khối (block) trên mạng lưới và được thưởng bằng token. Mỗi giao dịch được mã hóa bằng một phương trình đòi hỏi sức mạnh tính toán lớn xử lí. Thợ đào giải phương trình đầu tiên cho phép giao dịch diễn ra và được thưởng một khoản phí nhỏ.

135. **Mining pool** – Một hệ thống phần mềm tập chung nhóm các thợ đào để có thể xác nhận khối (block) và xử lí giao dịch nhiều hơn. Lợi nhuận sẽ được phân chia cho các thành viên trong nhóm.

136. **Node** – Một máy tính kết nối với hệ thống và giữ một bản sao lưu của sổ cái Blokchain.

137. **Paper wallet** – Một trong những biện pháp bảo mật lưu trữ cryptocurrency trong môi trường ngoại tuyến (Cold storage). Ví giấy có thể được in ra trên bất kỳ

máy in nào, bao gồm khóa công cộng và khóa riêng tư duy nhất của người dùng, được mã hóa dưới dạng mã QR. Người dùng muốn giao dịch cần phải quét ví giấy.

138. **Peer-to-Peer (P2P)** – Hành động chia sẻ thông tin trực tiếp giữa hai bên trên một mạng nhất định mà không cần một máy chủ trung gian để truyền dữ liệu.

139. **Private Key** – Khóa bảo mật riêng tư là một dạng mã hóa cryptocurrency. Mỗi người dùng trên mạng đều có khóa bảo mật riêng tư, tương đương như mật khẩu để truy cập vào tài khoản.

140. Đây là một ví dụ cho Private Key: 3a1076bf45ab87712ad64ccb3b10217737f7faacbf2872e88fdd9a537d8fe266

141. **Proof of Stake (PoS) **– Một thuật toán về việc chứng minh cổ phần, xác định người dùng nào đủ điều kiện xác nhận khối vào Blockchain, để kiếm được một khoản phí khai thác. Những người có nhiều token hơn sẽ được ưu tiên hơn những người có ít token.

142. **Proof of Work (PoW)** – Một thuật toán về việc chứng minh bằng công, xác định người dùng nào đủ điều kiện xác nhận khối vào Blockchain, để kiếm được một khoản phí khai thác giống với PoS. Tuy nhiên với PoW, tính đủ điều kiện được xác định qua sức mạnh tính toán chứ không phải số lượng tài sản của thợ mỏ.

143. **Public Key** – Là một đoạn mã (hay địa chỉ) cho phép nhận cryptocurrency từ người gửi.

144. Đây là một ví dụ cho Public Key: 0xC2D7CF95645D33006175B78989035C7c9061d3F9

145. **SegWit** – Viết tắt của “Segregated Witness”, là một bản cập nhật được đề xuất cho phần mềm Bitcoin, Segwit ra đời với mục đích vá lỗi các vấn đề nghiêm trọng và cải thiện một số các chức năng. Có thể coi SegWit là một trường hợp Soft Fork.

146. **Smart Contract **– Một thuật toán sử dụng công nghệ Blockchain để tự động thực hiện một hợp đồng. Các điều khoản của một hợp đồng thông minh được thực hiện khi các bên tham gia đáp ứng tất cả các yêu cầu. Hợp đồng thông minh được phổ biến bởi mạng lưới Ethereum.

147. **Token** – Loại tiền tệ đại diện của một mạng Blockchain, mang lại giá trị thông qua các giao dịch trên mạng lưới.

148. Ví dụ: Token của Bitcoin kí hiệu là BTC, Token của Cardano kí hiệu là ADA,…

149. **Transaction Fee** – Phí giao dịch. Vì các giao dịch trên một mạng Blockchain đòi hỏi sức mạnh tính toán đáng kể, các thợ mỏ trên mạng lưới cạnh tranh cho quyền xử lý giao dịch. Thợ mỏ đầu tiên xử lý sẽ nhận phí giao dịch.

150. **Wallet** – Ví là một chương trình trực tuyến cho phép người dùng lưu trữ, chuyển và xem số dư trong tài khoản. Các ví khác nhau sẽ hỗ trợ các loại cryptocurrency khác nhau. Một số ví hỗ trợ nhiều loại cryptocurrency trên một nền tảng duy nhất.

151. **Whitepaper** – Một bản báo cáo mô tả chi tiết về dự án ICO (Initial Coin Offering) của một công ty hay một nhóm nhà phát triển sẽ thực hiện, giúp nhà đầu tư có một cái nhìn tổng quan về dự án, từ đó đưa ra quyết định đầu tư.