Họ Tên:..... MSSV:.....	**ĐỀ KIỂM TRA CUỐI KỲ** **MÔN MẬT MÃ & AN NINH MẠNG** **Ngày thi: 31/05/2018 - Thời gian: 90 phút**

Ghi chú:

- *Sinh viên **không** được phép sử dụng tài liệu*
- *Mỗi câu hỏi trắc nghiệm, **chỉ chọn một câu trả lời đúng nhất***
- *Sinh viên phải sử dụng giấy trả lời trắc nghiệm cho phần trả lời câu hỏi trắc nghiệm*
- ***Sinh viên phải ghi tên và MSSV lên đề thi và nộp trở lại***

Câu 1. Một đoạn mã độc được đính vào tập tin khác để thực hiện việc nhân bản, có thể là
A. Worm **B.** Virus
C. Logic bomb **D.** Trojan

Câu 2. Tại sao hackers muốn che giấu dấu vết?
A. Để ngăn ngừa kẻ khác dùng những chương trình mình đã cài đặt trong hệ thống nạn nhân
B. Để ngăn ngừa phát hiện hoặc điều tra
C. Để ngăn ngừa sự xâm nhập
D. Để không cho những hackers khác dùng công cụ của mình

Câu 3. Một loại công nghệ có thể được dùng để mã hóa giao tiếp (encrypt communication) từ điểm A đến điểm B trong mạng *không tin cậy về bảo mật*:
A. VPN **B.** VLAN
C. NAP **D.** NAT

Câu 4. Hacker có thể lấy được mật khẩu mà không phải sử dụng bất cứ công cụ hay chương trình máy tính nào, thông qua kỹ thuật
A. Backdoors **B.** Sniffers
C. Social Engineering **D.** Trojan Horses

Câu 5. Hệ thống của bạn bị đứng (stop responding) khi gõ lệnh từ bàn phím. Bạn ghi nhận việc này cứ sau mỗi lần mở file Excel và kết nối Internet. Có thể bạn là nạn nhân của kiểu tấn công sử dụng:
A. Virus **B.** Worm
C. ARP Poisoning **D.** Logic bomb

Câu 6. Kiểu tấn công khi kẻ gian khai thác điểm yếu để can thiệp vào cơ sở dữ liệu gọi là:
A. SQL tearing **B.** SQL manipulation
C. SQL cracking **D.** SQL injection

Câu 7. Tấn công đoán mật khẩu dựa vào tự điển (dictionary attack) là dạng tấn công
A. Dùng thuật toán và các giải thuật xử lý song song
B. Dùng giải thuật RSA để thực hiện
C. Sử dụng thuật toán brute force để đoán mật khẩu người dùng
D. Thử lần lượt và tuần tự các giá trị đã được khai báo trước

Câu 8. Phát biểu nào sau đây KHÔNG là một trong những mục đích của việc quét (scanning) trong mạng máy tính:
A. Tìm những cổng mở (open ports) **B.** Tìm những dịch vụ chạy trên servers mục tiêu
C. Xác định hệ điều hành **D.** Thu thập số phone của nhân viên

Câu 9. Giải thuật RSA khác giải thuật DES (Data Encryption Standard) ở chỗ
A. Nó không thể tạo ra được chữ ký số **B.** Nó dùng khóa công khai để mã hóa
C. Nó dựa trên giải thuật mã hóa khóa đối xứng **D.** Tất cả các câu trả lời trên đều sai

Câu 10. Chọn câu trả lời đúng cho một loại công nghệ cho phép kết nối được thiết lập giữa hai mạng máy tính sử dụng giao thức bảo mật:

A. Tunneling
B. VLAN
C. Internet
D. Extranet

Câu 11. Một thông điệp như sau được gửi đi "I love you", bên nhận nhận được thông điệp có nội dung là "I don't love you", quá trình truyền thông tin đã bị 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 sẵn sàng

Câu 12. Cụm từ viết tắt CIA trong an ninh mạng, được dùng để nói về:

A. Certificate, Integrity, Authentication
B. Certificate, Integrity, Availability
C. Confidentiality, Inspection, Authentication
D. Confidentiality, Integrity, Availability

Câu 13. Mặt hạn chế của mã hóa đối xứng là:

A. nó dễ dàng bị kẻ gian giải mã
B. nó chạy quá chậm nên khó có thể được dùng trên thiết bị di động
C. nó đòi hỏi khóa chung đươc chia sẻ một cách bí mật
D. nó chỉ được dùng trên Unix

Câu 14. Mã hóa bất đối xứng có ưu điểm nào so với mã hóa đối xứng?

A. An toàn hơn (more secure)
B. Giải thuật có cả vai trò quản lý khóa (key management)
C. Bất cứ ai có khóa công cộng đều có thể giải mã dữ liệu.
D. Nó dùng hàm băm

Câu 15. Chữ ký số (digital signature) dùng loại mã hóa nào sau đây?

A. Hashing và asymmetric
B. Asymmetric và symmetric
C. Hashing và symmetric
D. Tất cả các câu trả lời trên đều sai

Câu 16. Mục đích của một DMZ trong một mạng là

A. Cung cấp những kết nối dễ dàng đến Internet mà không làm ảnh hưởng firewall
B. Cho phép những cụm máy chủ (server farms) được chia nhỏ thành những đơn vị có chức năng tương tự nhau
C. Cung cấp một nơi cài bẫy và bắt giữ hackers
D. Thực hiện vai trò như một vùng đệm giữa những mạng tin cậy (trusted networks) và không tin cậy (untrusted networks)

Câu 17. SYN flood là một ví dụ cho kiểu tấn công nào?

A. Mã độc
B. Từ chối dịch vụ
C. Man-in-the-middle
D. Đánh lừa (spoofing)

Câu 18. Cuộc tấn công trong đó kẻ tấn công đơn giản chỉ lắng nghe dòng dữ liệu với hy vọng sẽ lấy được thông tin nào đó, như User ID, số thẻ tín dụng, v.v., được gọi là

A. A man-in-the-middle attack
B. A denial-of-service-attack
C. A sniffing attack
D. A backdoor attack

Câu 19. Kẻ tấn công gởi lại những câu lệnh (command) và mã (codes) dùng trong giao dịch tài chính để hòng thực hiện nhiều lần giao dịch ấy, kiểu tấn công này thuộc dạng:

A. Spoofing
B. Man-in-the-middle
C. Replay
D. Backdoor

Câu 20. SSL có thể được dùng để bảo mật cho

A. POP3 traffic
B. HTTP traffic
C. SMTP traffic
D. Tất cả các câu trả lời trên đều đúng

Câu 21. SSL KHÔNG cung cấp chức năng nào sau đây?
A. Toàn vẹn dữ liệu (Data integrity services)
B. Xác thực (Authentication services)
C. Bí mật dữ liệu (Data confidentiality services)
D. Tính sẵn sàng của dữ liệu (Availability of data)

Câu 22. SSL dùng cổng nào để mang HTTPS traffic?
A. TCP port 80
B. UDP port 443
C. TCP port 443
D. TCP port 8080

Câu 23. _____ là quá trình kiểm chứng hoặc kiểm thử tính hợp lệ của định danh khai báo.
A. Identification
B. Authentication
C. Authorization
D. Accountability

Câu 24. Hệ thống phát hiện xâm nhập (IDS) được thiết kế chủ yếu để thực hiện chức năng nào?
A. Phát hiện hành vi bất thường (Detect abnormal activity).
B. Phát hiện hư hỏng hệ thống (Detect system failures).
C. Đánh giá hiệu năng hệ thống (Rate system performance).
D. Kiểm thử hệ thống để phát hiện điểm yếu (Test a system for vulnerabilities)

Câu 25. Cuộc tấn công khi kẻ gian tự đặt vị trí của mình giữa Client và Server, làm gián đoạn giao dịch và chiếm quyền giao dịch này, được gọi là cuộc tấn công:
A. Man-in-the-middle
B. Spoofing
C. Session Hijacking
D. Cracking

Câu 26. Câu trả lời nào sau đây KHÔNG được xem là xâm phạm tính bí mật (confidentiality)?
A. Trộm password (stealing passwords)
B. Nghe trộm (eavesdropping)
C. Phá hoại phần cứng (hardware destruction)
D. Man-in-the-middle

Câu 27. Loại cipher nào khi thay đổi vị trí các ký tự bên trong thông điệp để tăng tính bảo mật
A. Stream cipher
B. Transposition cipher
C. Block cipher
D. Substitution cipher

Câu 28. Dùng phương pháp mã hóa hoán vị Rail Fence với depth 2, thông điệp "I MUST PASS THIS EXAM" hãy cho biết, sau khi mã hóa, thông điệp sẽ là gì?
A. IMUSTPASSTHISEXAM
B. IUTASHSXMMSPSTIEA
C. IUMSTAPSSHTISXEAM
D. MAXESIHTSSAPTSUMI

Câu 29. Trong phương pháp dùng khóa bất đối xứng, Alice muốn ký chữ ký số (digital signature) và người nhận là Bob. Để đọc chữ ký số này, Bob phải dùng đến
A. public-key của Alice
B. public-key của Bob
C. private-key của Alice
D. private-key của Bob

Câu 30. Trong phương pháp dùng khóa bất đối xứng, Alice muốn gởi thông điệp bí mật và người nhận là Bob. Để thực hiện việc này, Alice phải dùng đến
A. public-key của Alice
B. public-key của Bob
C. private-key của Alice
D. private-key của Bob

Câu 31. Chọn câu trả lời đúng cho một phương pháp cổ điển mã hóa dùng giải thuật thay thế (substitution):
A. Rivest, Shamir, Adleman (RSA)
B. Data Encryption Standard (DES)
C. Rail Fence
D. Tất cả các câu trả lời trên đều sai

Câu 32. Mục tiêu của tường lửa là gì?
A. Bảo vệ một mạng máy tính trước các nguy cơ bảo mật từ bên ngoài
B. Ngăn chặn dữ liệu lưu thông ra khỏi mạng.
C. Block SNA traffic (Systems Network Architecture)
D. Giám sát lưu thông mạng (Monitor network Traffic)

Câu 33. Một dạng tấn công dựa vào xác suất 2 thông điệp khác nhau dùng hàm băm giống nhau để cho ra giá trị giống nhau gọi là
A. Birthday attack
B. Statistic attack
C. Differential cryptanalysis attack
D. Known ciphertext attack

Câu 34. Dùng Caesar cipher, mã hóa thông điệp "I will pass this exam", kết quả sẽ là:
A. L zloo sdvv wklv hadp
B. M ampp texx xlmw ibeq
C. N bnqq ufyy jcfr
D. Tất cả các câu trả lời trên đều sai

Câu 35. Để chống lại một cuộc tấn công thụ động (passive attack), người ta thường
A. tìm cách phát hiện (detect) ra cuộc tấn công, sau đó xử lý nó
B. tìm cách ngăn ngừa (prevent) cuộc tấn công này
C. không làm gì cả (vì đây chỉ là cuộc tấn công thụ động)
D. Tất cả các câu trả lời trên đều sai

Câu 36. Microsoft Windows dùng protocol nào sau đây để thực hiện lệnh tracert?
A. ICMP
B. ARP
C. UDP
D. FTP

Câu 37. Kiểu tấn brute-force khai thác điểm yếu của
A. Khóa (dùng mã hóa dữ liệu)
B. Giải thuật (dùng mã hóa dữ liệu)
C. Cả 2 câu trả lời A và B đều đúng
D. Cả 2 câu trả lời A và B đều sai

Câu 38. Ngay khi phát hiện hệ thống đã bị xâm nhập trái phép, để quá trình thu thập những bằng chứng có hiệu quả và có độ tin cậy cao, hành động nào sau đây phải được ưu tiên thực hiện trước nhất
A. Dump bộ nhớ của hệ thống ra file
B. Cách ly hệ thống khỏi mạng
C. Tạo disk image cho hệ thống bị xâm nhập
D. Khởi động lại hệ thống

Câu 39. Những biện pháp nào dưới đây không giúp chống lại những phần mềm độc hại?
A. Bộ lọc chống spam
B. Phần mềm phòng chống spyware
C. Chính sách cho việc cài đặt những patch
D. Sử dụng password

Câu 40. Những ví dụ nào dưới đây ảnh hưởng tới tính bí mật thông tin của tổ chức?
A. Làm giả dữ liệu
B. Sử dụng dữ liệu cho mục đích cá nhân
C. Mất cắp
D. Tai nạn do xóa nhầm dữ liệu

Câu 41. Nghe trộm thuộc kiểu tấn công
A. Active
B. Passive
C. Aggressive
D. Masquerading

Câu 42. Xác thực thông điệp (Message authentication) là một cơ chế hoặc dịch vụ, dùng để kiểm tra
A. tính toàn vẹn của thông điệp
B. tính bí mật của thông điệp
C. tính sẵn sàng của thông điệp
D. Tất cả các câu trả lời trên đều sai

Câu 43. Steganography là một kỹ thuật dùng để
A. phát hiện giải thuật mã hóa mà người khác đã dùng thông qua ciphertext
B. giấu một thông điệp bên trong một thông điệp khác, như file văn bản, hình ảnh, audio, video, ...
C. truy tìm tất cả các khả năng của khóa
D. Tất cả các câu trả lời đều sai

Câu 44. Chọn câu trả lời đúng cho mục tiêu của sinh trắc học (biometrics) trong kiểm soát truy cập:
A. Authorization
B. Availability
C. Authentication
D. Accountability

Câu 45. Hàm băm (hash function) là hàm, thỏa mãn các điều kiện sau:
A. input có thể có độ dài khác nhau, cho ra output có độ dài bằng với input tương ứng
B. input có thể có độ dài khác nhau, cho ra output cũng có độ dài khác nhau
C. input có độ dài bằng nhau, cho ra output có độ dài khác nhau
D. input có thể có độ dài khác nhau, cho ra output có độ dài bằng nhau

Câu 46. Yêu cầu cơ bản cần thiết đối với chữ ký số (digital signature) là gì?
A. Có giá trị phụ thuộc vào thông điệp đã ký
B. Dùng thông tin mà duy nhất người ký biết
C. Không thể giả mạo được (về mặt tính toán)
D. Tất cả các câu trả lời trên đều đúng

Câu 47. Khái niệm zombie trong an ninh mạng được chỉ đến
A. Máy tính của hacker
B. Mục tiêu chính của cuộc tấn công DDoS
C. Một hệ thống các host bị hại, và cũng là mục tiêu chính của cuộc tấn công DDoS
D. Một hệ thống bị hại, không là mục tiêu chính, được dùng để thực hiện cuộc tấn công DDoS

Câu 48. Bạn nhận được tín hiệu báo động, trên server trong mạng máy tính có một chương trình đang chạy trái phép (bypass authorization). Cuộc tấn công nào đang được nói đến?
A. Deface Attack
B. DDoS
C. Backdoor
D. Social engineering

Câu 49. Kiểu tấn công Buffer Overflow được thực hiện bằng cách:
A. tác động làm tràn buffer của các thiết bị mạng, như router
B. tác động làm tràn bộ nhớ của biến trong đoạn code chương trình
C. tác động làm cho mục tiêu không còn đủ tài nguyên để đáp ứng yêu cầu của client
D. Tất cả các câu trả lời trên đều sai

Câu 50. Chữ ký số cung cấp thành phần bảo mật nào?
A. Cung cấp khả năng mã hóa dữ liệu mật của cá nhân
B. Đảm bảo tính riêng tư của cá nhân
C. Chỉ ra nguồn dữ liệu và xác minh tính toàn vẹn dữ liệu
D. Cung cấp framework về luật và quy trình

Câu 51. Trong lĩnh vực mạng máy tính, cổng (port) được dùng để xác định:
A. Địa chỉ của một ứng dụng trên Internet
B. Địa chỉ của một máy tính trên Internet
C. Địa chỉ của một ứng dụng trên một máy tính
D. Tất cả các câu trả lời trên đều sai

Câu 52. Chọn câu trả lời đúng cho công cụ phù hợp nhất dùng để mã hóa thư điện tử:
A. SSH
B. IPSEC
C. TLS
D. PGP

Câu 53. Chữ ký tay trên tài liệu giấy thuộc kiểu xác thực nào sau đây:
A. Xác thực dựa trên điều người dùng biết
B. Xác thực dựa trên điều người dùng có
C. Xác thực dựa trên yếu tố sinh trắc học
D. Tất cả các câu trả lời trên đều sai

Câu 54. Trong các đáp án dưới đây, đáp án nào KHÔNG đúng?
A. 1 xor 1 = 1
B. 0 xor 0 = 0
C. 1 xor 0 = 1
D. 0 xor 1 = 1

Câu 55. Chọn câu trả lời đúng cho một đoạn mã độc được giấu bên trong một chương trình hữu dụng, không có khả năng tự nhân bản:
A. Worm
B. Virus
C. Trojan
D. Tất cả các câu trả lời trên đều sai

Câu 56. Cuộc tấn công khi kẻ gian giả làm người dùng hợp lệ và tạo kết nối đến server gọi là

A. Session hijacking **B.** DDoS
C. Spoofing **D.** Social Engineering

Câu 57. Công cụ nào sau đây được dùng nhiều nhất được dùng để đọc tập tin logs lớn để tìm kiếm những vấn đề liên quan đến xâm nhập:

A. Text editor **B.** Vulnerability scanner
C. Password cracker **D.** IDS

Câu 58. Dùng DES (Data Encryption Standard), input plaintext block có độ dài là

A. 32 bit **B.** 56 bit
C. 64 bit **D.** 128 bit

Câu 59. Virus không thể xâm nhập vào thành phần nào sau đây của một hệ thống:

A. File **B.** System sectors
C. Memory **D.** DLL files

Câu 60. Để phát hiện tấn công an ninh mạng trên một hệ thống đơn lẻ, thành phần nào sau đây có thể được dùng đến

A. Firewall **B.** Honeypot
C. NIPS **D.** HIDS

==========

Ban chủ nhiệm Khoa

Giáo viên ra đề

Nguyễn Đức Thái