HỌC VIỆN KTMM
PHÒNG KT&ĐBCLĐT

ĐỀ THI CHÍNH THỨC
(Đề thi có 6 trang)

ĐỀ THI MẪU ĐỂ CÔNG BỐ
Môn thi: CƠ SỞ ATTT
Thời gian làm bài: 60 phút, không kể thời gian phát đề

Họ, tên thí sinh: .....
Số báo danh: .....

Mã đề thi 965

Câu 1. Tường lửa nào sau đây theo dõi trạng thái hoạt động và đặc điểm của các kết nối mạng đi qua nó?

A. Tường lửa trạng thái
B. Tường lửa phi trạng thái
C. Tường lửa lọc gói
D. Tường lửa ứng dụng

Câu 2. Một chương trình hoặc tiến trình lưu trữ nhiều dữ liệu hơn trong vùng lưu trữ dữ liệu tạm thời so với dự định lưu trữ được gọi là tình huống nào sau đây?

A. Tràn bộ đệm
B. Quá tải bộ nhớ
C. Từ chối dịch vụ
D. Từ chối dịch vụ phân tán

Câu 3. Một người dùng trên mạng nhận được e-mail từ ngân hàng nói rằng đã có sự cố an ninh tại ngân hàng. Email tiếp theo yêu cầu người dùng đăng nhập vào tài khoản ngân hàng theo liên kết được cung cấp để xác minh tài khoản. Đây có thể là loại tấn công nào?

A. Dictionary attack **B**. Spam **C**. Phishing **D**. Spim

Câu 4. Thuật toán nào sau đây không phải là ví dụ của thuật toán mã hóa đối xứng?

A. AES **B**. Rijndael **C**. Diffie-Hellman **D**. RC6

Câu 5. Giải pháp nào sau đây là giải pháp tốt nhất để duy trì hoạt động máy tính khi xảy ra sự cố mất điện?

A. Nguồn cấp điện kép
B. UPS
C. Máy phát điện
D. Nguồn điện dự phòng

Câu 6. Các nhà phát triển web tại công ty đang thử nghiệm mã trang web mới nhất trước khi đi vào hoạt động để đảm bảo rằng nó hoạt động hiệu quả và an toàn. Trong quá trình thử nghiệm, họ thử các URL không đúng định dạng với các tham số bất thường và dữ liệu ngẫu nhiên. Thuật ngữ nào mô tả hành động trên?

A. Debugging
B. Cross-site scripting
C. Fuzzing
D. Patching

Câu 7. Loại phần mềm độc hại nào sau đây sẽ hữu ích và khó bị phát hiện nhất trong các cuộc tấn công leo thang đặc quyền?

A. Worm **B**. Ransomware **C**. Rootkit **D**. RAT

Câu 8. Những phát biểu nào sau đây là ĐÚNG?

A. ISO 27001 là một tiêu chuẩn xác định các yêu cầu đối với hệ thống bảo vệ thông tin.
B. ISO 27001 là một tiêu chuẩn xác định các rủi ro đối với hệ thống quản lý an toàn thông tin.
C. ISO 27001 là một bộ các tiêu chuẩn quốc tế về quản lý an toàn thông tin
D. ISO 27001 là một tiêu chuẩn về an toàn thông tin

Câu 9. Lý do nào giải thích ĐÚNG NHẤT tại sao cần sử dụng hàm băm trong chữ ký số:

A. Tăng độ an toàn chữ ký số

B. Giảm kích thước chữ ký số

C. Đảm bảo tính chống chối bỏ

D. Không thể thiếu được trong sơ đồ chữ ký số

Câu 10. Tại Việt Nam, cơ quan nào chịu trách nhiệm điều phối quốc gia về ứng cứu sự cố an toàn thông tin?

A. Trung tâm an ninh mạng GSEC

B. Trung tâm an ninh mạng VSEC

C. Trung tâm an ninh mạng VNISA

D. Trung tâm VNCERT

Câu 11. Giải pháp nào nên sử dụng bảo vệ lưu lượng mạng của dịch vụ web?

A. MD5

B. SHA-256

C. HTTPS

D. SHA-512

Câu 12. Bạn thiết lập chính sách an toàn yêu cầu người dùng bảo vệ tất cả các tài liệu giấy để dữ liệu nhạy cảm của khách hàng, nhà cung cấp hoặc công ty không bị đánh cắp. Đây là loại chính sách nào?

A. Quyền riêng tư (privacy)

B. Mật khẩu (password)

C. Sử dụng được chấp nhận (Acceptable use)

D. Bàn làm việc sạch sẽ (Clean desk)

Câu 13. Kẻ tấn công đã liên hệ với một trong những nhân viên và đã thuyết anh ta sử dụng tên người dùng và mật khẩu của mình, cho phép kẻ tấn công truy cập vào hệ thống mạng. Đây là kiểu tấn công nào?

A. Social engineering

B. HIDS/HIPS

C. Data exfiltration

D. Permission issues

Câu 14. Để tuân thủ các nguyên tắc bảo mật mới của công ty, các chi nhánh cần phải theo dõi thông tin chi tiết về các trang web nhân viên đã truy cập. Bạn nên cài đặt những gì?

A. Proxy server

B. NIDS

C. VPN

D. Packet-filtering firewall

Câu 15. Điều nào sau đây là đúng về mật mã?

A. Mật mã khối thực hiện mã các khối dữ liệu.

B. Mật mã dòng thực hiện mã lưu lượng truyền trực tuyến

C. Mật mã dòng thực hiện mã dữ liệu từng 128 bytes một.

D. Mật mã khối phân tích các mẫu dữ liệu và chặn dữ liệu độc hại được mã hóa.

Câu 16. Phương án nào sau đây giúp phục hồi và đảm tính sẵn sàng của hệ thống?

A. File server backups

B. Smartcard authentication

C. Auditing

D. Testing

Câu 17. Người dùng chỉ nên được cấp quyền cần thiết để thực hiện các nhiệm vụ của họ?

A. Ủy quyền

B. Nguyên tắc đặc quyền tối thiểu

C. Tách nhiệm vụ

D. Trách nhiệm giải trình

Câu 18. Cho hàm băm H, từ H(x) không thể tìm được x là tính chất nào của hàm băm

A. Kháng tiền ảnh **B**. Kháng va chạm

C. Kháng tiền ảnh thứ 2 **D**. Nén

Câu 19. Ma trận kiểm soát truy cập (Acess Control Matrix) thể hiện mô hình kiểm soát truy cập nào?

A. Kiểm soát truy cập bắt buộc (MAC)

B. Kiểm soát truy cập dựa trên thuộc tính (ABAC)

C. Kiểm soát truy cập tùy chọn (DAC)

D. Kiểm soát truy cập dựa trên vai trò (RBAC)

Câu 20. Điều nào sau đây thể hiện **TỐT NHẤT** nguyên tắc đặc quyền tối thiểu?

A. Luôn sử dụng quyền quản trị viên để truy cập hệ thống

B. Gán cho người dùng toàn quyền kiểm soát tài nguyên mạng

C. Gán các quyền cần thiết để cho phép người dùng hoàn thành nhiệm vụ

D. Phát hiện phần mềm độc hại đang chạy mà không có đặc quyền nâng cao

Câu 21. Kisten muốn lưu trữ mật khẩu một cách an toàn bằng cách sử dụng hàm băm để chống lại cuộc tấn công vét cạn. Lựa chọn nào sau đây là TỐT NHẤT?

A. Bcrypt **B**. MD5 **C**. RC4 **D**. SHA1

Câu 22. Phương thức nào sau đây khiến thông tin nhạy cảm của tổ chức có thể bị rò rỉ ngoài ý muốn?

A. Ứng dụng mạng xã hội trên điện thoại di động

B. Quyền đối với tệp NTFS

C. Mã hóa tệp tin

D. Sao lưu đám mây được mã hóa

Câu 23. Người dùng mở tài liệu song khi mở ra thấy bên trong chỉ có các ký tự lạ vô nghĩa trong khi hôm trước tài liệu vẫn mở được nội dung bình thường. Khả năng người dùng rất có thể là nạn nhân của loại phần mềm độc hại nào dưới đây?

A. RAT **B**. Backdoor **C**. Crypto-malware **D**. Virus

Câu 24. Giả mạo IP thường được sử dụng cho loại tấn công nào sau đây?

A. Tấn công từ chối dịch vụ **B**. Tấn công Salami

C. Tấn công thu thập dữ liệu **D**. Tấn công ghi lại lịch sử phím gõ

Câu 25. Tính chất nào không được đảm bảo trong mạng VPN?

A. Mã hóa **B**. Xác thực **C**. Toàn vẹn **D**. Chống chối bỏ

Câu 26. Tấn công XSS (Cross Site Scripting) xuất hiện ở tầng nào?

A. Tầng ứng dụng – Application Layer **B**. Tầng mạng – Network Layer

C. Tầng trình diễn – Presentation Layer **D**. Tầng phiên – Session Layer

Câu 27. Quản trị viên có thể sử dụng cách nào sau đây để xác định xem có ai sử dụng trái phép mạng LAN không dây hay không?

A. Performance Monitor **B**. Wireless access point log

C. Proxy server **D**. Protocol analyzer

Câu 28. Chuyên gia bảo mật nhận thấy rằng một số cổng trong khoảng 8100-8200 đang lắng nghe trên một máy chủ web. Tuy nhiên, người chủ sở hữu hệ thống cho biết ứng dụng chỉ sử dụng cổng 443. Khuyến cáo nào sau đây là TỐT NHẤT cho người chủ hữu để giảm thiểu khả năng hệ thống bị tấn công?

A. Chuyển ứng dụng sang cổng khác

B. Tắt các dịch vụ không cần thiết

C. Lọc cổng 443 cho các địa chỉ IP cụ thể

D. Giám sát lưu lượng trên cổng 443

Câu 29. Các thiết bị hay phần mềm để đảm bảo an toàn nào sau đây nên được sử dụng để theo dõi và cảnh báo tới người quản trị mạng về xâm nhập trái phép?

A. IDS **B**. Switch

C. Antivirus **D**. Công cụ phân tích mạng

Câu 30. Loại kiểm thử an toàn nào cung cấp thông tin cấu hình mạng cho người kiểm tra?

A. Gray box **B**. White box

C. Black box **D**. Blue box

Câu 31. Trình tự nào sau đây là ĐÚNG?

A. Định danh → Xác thực → Cấp quyền **B**. Xác thực → Định danh → Cấp quyền

C. Cấp quyền → Xác thực → Định danh **D**. Định danh → Cấp quyền → Xác thực

Câu 32. Một quản trị viên bị sa thải, 30 ngày sau, máy chủ chứa dữ liệu nội bộ và máy chủ dự phòng của tổ chức gặp sự cố đồng thời cùng một lúc. Kiểm tra các máy chủ, có vẻ như các tệp hệ thống quan trọng đã bị xóa khỏi cả hai máy chủ. Nếu quản trị viên chịu trách nhiệm quản lý các máy chủ đó trong thời gian làm việc thì đây rất có thể là một ví dụ về loại mã độc nào?

A. Crypto-malware **B**. Logic bomb **C**. Worm **D**. Trojan

Câu 33. Tuấn đang nghiên cứu các kỹ thuật được sử dụng bởi tin tặc. Tuấn quyết định gửi một gói tin đến hệ thống mục tiêu, nhưng thay đổi địa chỉ IP nguồn của gói tin để có vẻ như nó đến từ người khác. Đây là kiểu tấn công nào?

A. Spim **B**. Pharming **C**. Spoofing **D**. Phishing

Câu 34. Phương pháp tốt nhất chống lại virus mới trên hệ điều hành Windows là gì?

A. Luôn cập nhật các mẫu mới cho phần mềm diệt virus

B. Sử dụng giải pháp mã hóa

C. Tắt máy tính khi không sử dụng

D. Không kết nối mạng Wifi

Câu 35. Sự khác biệt giữa đánh giá rủi ro và quản lý rủi ro là gì?

A. Quản lý rủi ro xác định và ưu tiên các rủi ro; đánh giá rủi ro là việc quản lý các rủi ro để giảm thiểu tác động của chúng.

B. Đánh giá rủi ro xác định các mối đe dọa; quản lý rủi ro kiểm soát các mối đe dọa đó.

C. Không có khác biệt

D. Đánh giá rủi ro xác định và ưu tiên các rủi ro; quản lý rủi ro là quản lý rủi ro để giảm thiểu tác động của chúng.

Câu 36. Thực hiện kiểm tra an toàn ứng dụng, loại kiểm tra nào sau đây liên quan đến việc nhập dữ liệu ngẫu nhiên, không đúng định dạng?

A. Fuzzing Testing
B. Buffer Overflow
C. XSS
D. Whitebox test

Câu 37. Cách TỐT NHẤT để chống trộm máy tính xách tay là gì?

A. GPS
B. Cable lock
C. Antivirus software
D. Host-based firewall

Câu 38. Tường lửa lọc gói tin sử dụng loại kiểm soát truy cập nào để cho phép hoặc từ chối lưu lượng mạng?

A. Kiểm soát truy cập tùy ý
B. Kiểm soát truy cập dựa trên luật
C. Kiểm soát truy cập dựa trên vai trò
D. Kiểm soát truy cập bắt buộc

Câu 39. Loại phần mềm nào kiểm tra hành vi, nhật ký và sự kiện của ứng dụng trên máy tính để tìm hoạt động đáng ngờ?

A. NIDS
B. Host-based firewall
C. Spyware
D. HIDS

Câu 40. Bạn nghi ngờ máy chủ DNS thực hiện chuyển hướng DNS sai tới các máy chủ trong một cuộc tấn công DDOS. Bạn nên sử dụng lệnh nào của hệ điều hành Windows để kiểm tra điều này?

A. arp **B**. ping **C**. nslookup **D**. netstat

Câu 41. Giải pháp nào sau đây đảm bảo an toàn cho việc truy cập một máy chủ từ xa?

A. SSO **B**. SSH **C**. SSL **D**. SHA

Câu 42. Bạn chịu trách nhiệm quản lý một máy chủ FTP nội bộ. Một người dùng báo cáo rằng các tệp có sẵn trên máy chủ không còn nữa. Bạn có thể tìm ở đâu để xác định điều gì đã xảy ra với các tệp bị thiếu?

A. Nhật ký tải lên FTP
B. Nhật ký tường lửa
C. Nhật ký tải xuống FTP
D. Nhật ký truy cập FTP

Câu 43. Loại phần mềm nào hoạt động chống lại việc thu thập thông tin trên máy tính?

A. Anti-spam **B**. Antispyware **C**. Anti-adware **D**. Antivirus

Câu 44. Tấn công APT là viết tắt của?

A. Advanced Persistent Tool
B. Advanced Persistent Threat
C. Applied Persistent Threat
D. Advanced Programmed Threat

Câu 45. Mô tả nào đúng về sự cố an toàn thông tin?

A. Các sự kiện vi phạm chính sách an toàn thông tin, hay thất bại trong biện pháp bảo vệ tài sản thông tin xảy ra trong hệ thống, dịch vụ hay mạng của tổ chức. Hoặc một tình trạng hay sự việc xảy ra có liên quan đến an toàn thông tin

B. Một hay một chuỗi các sự kiện an toàn thông tin không mong muốn hay bất ngờ xảy ra gây tổn hại nghiêm trọng đến hoạt động kinh doanh và đe dọa đến đến vấn đề an ninh thông tin

C. Các hành động tấn công mạng nhằm vào hệ thống

D. Hệ thống quản lý an toàn thông tin

Câu 46. Trong mô hình MAC. Biểu thức thể hiện tính trội nào dưới đây là ĐÚNG?

A. (2, Kinh doanh) ≤ (3, (Kinh doanh, Lập trình viên))

B. (3, Kinh doanh, Hành chính) ≤ (2, (Kinh doanh, Lập trình viên))

C. (2, (Kinh doanh, Lập trình viên)) ≤ (3, Kinh doanh)

D. (3, Kinh doanh) ≤ (2, (Hành chính, Lập trình viên))

Câu 47. Chức năng của mạng Honeynet là gì?

A. Kiểm soát mạng dựa vào tập luật có sẵn

B. Phân tích, cảnh báo và ngăn chặn mã độc dựa trên mẫu

C. Phát hiện và ngăn chặn xâm nhập

D. Thu hút, phân tích và cảnh báo xâm nhập

Câu 48. Đáp án nào sau đây mô tả đúng nhất về kiểu tấn công được thiết kế để làm ngừng hoạt động mạng bằng cách làm gián đoạn hệ thống với lưu lượng vô ích?

A. Ping of death

B. Denial of Service

C. Teardrop

D. Social engineering

Câu 49. Cách nào sau đây là tốt nhất và đơn giản nhất để chống lại lỗ hổng trong hệ điều hành?

A. Cài đặt bản vá mới nhất

B. Cài đặt lại hệ điều hành thông dụng

C. Sao lưu hệ thống thường xuyên

D. Tắt hệ thống khi không sử dụng

Câu 50. Sau khi cài đặt một phần mềm mới từ một trang web trực tuyến và sau đó xem lại nhật ký hệ thống, bạn nhận thấy rằng chương trình đã chạy mà không có sự đồng ý của bạn. Bạn cũng nhận ra rằng các tệp cũng đã được thêm và xóa vào những lúc bạn không sử dụng máy tính. Công cụ nào sau đây có nhiều khả năng được sử dụng?

A. Backdoor

B. Logic bomb

C. Virus

D. Phần mềm quảng cáo

---------- *Hết* ----------