TRƯỜNG ĐẠI HỌC NGÂN HÀNG TP.HCM
KHOA HỆ THỐNG THÔNG TIN QUẢN LÝ

ĐỀ THI KẾT THÚC HỌC PHẦN
MÔN: AN TOÀN BẢO MẬT THÔNG TIN
(số câu trong đề thi: 53)
Thời gian làm bài: 60 phút

Họ và tên : …….. MSSV: ……..

NỘI DUNG ĐỀ THI

Câu 1.
Chỉ số port của dịch vụ HTTPS là bao nhiêu?
a. 80
b. 119
c. 143
d. 443

Câu 2.
Hai người A và B sử dụng chữ ký số trong các bức điện giao dịch với nhau. Trong đó K1 là khóa mật của A, K2 là khóa công khai của A, K3 là khóa mật của B, K4 là khóa công khai của B. Nếu A gửi cho B 1 bức điện có chữ ký số thì B sẽ phải dùng khóa nào để xử lý bức điện đó?
a. K1
b. K2
c. K3
d. K4

Câu 3.
Phương pháp điều khiển truy cập nào có liên quan đến vai trò của một cá nhân trong tổ chức?
a. MAC
b. DAC
c. RBAC
d. STAC

Câu 4.
Phương pháp truy cập nào sau đây dựa trên các truy cập được thiết lập trước và người sử dụng không thể thay đổi?
a. Kerberos
b. RBAC (Role-Based Access Control)
c. DAC (Discretionary Access Control)
d. MAC (Mandatory Access Control)

Câu 5.
Đối với hoạt động bảo mật cổng tòa nhà, ta nên thực hiện
a. Chia các vùng bảo mật
b. Lắp đặt khóa, camera an ninh
c. Triển khai các hệ thống báo cháy, trộm
d. Cả ba câu trên đều đúng

Câu 6.
Mô hình tin cậy được sử dụng với PKI có bao nhiêu phân loại?
a. 2
b. 3
c. 4
d. 5

Câu 7.
Quy trình tạo khóa mới để thay thế các khóa hết hạn gọi là gì?
a. Key renewal
b. Rollover

c. Archival
d. Revocation

Câu 8.
Chọn phát biểu đúng về hàm băm (hashing)?
a. Là quá trình chuyển đổi một thông điệp, hoặc dữ liệu thành bản tóm lượt giá trị số học
b. Là quá trình giải mã một thông điệp, hoặc dữ liệu
c. Là một thuật toán tạo khóa mã hóa
d. Là một thuật toán tạo khóa giải mã

Câu 9.
Chính sách nào chỉ ra chi tiết độ nhạy cảm và cách sử dụng thông tin?
a. Chính sách bảo mật
b. Chính sách phân loại thông tin
c. Chính sách cách sử dụng
d. Chính sách quản trị cấu hình

Câu 10.
Chính sách nào quy định cách quản lý chứng nhận và chấp nhận chứng nhận?
a. Chính sách chứng nhận
b. Danh sách truy xuất chứng nhận
c. CA công nhận
d. Luật CRL

Câu 11.
Trong bảo mật thông tin, chúng ta có nhiêu tầng?
a. 1
b. 2
c. 3
d. 4

Câu 12.
Địa chỉ port một dịch vụ do server cung cấp là giá trị
a. Cố định
b. Thay đổi thường xuyên
c. Thay đổi định kỳ
d. Cả ba câu trên đều sai

Câu 13.
Quá trình đưa ra phản ứng đối với hành động tấn công được gọi là gì?
a. Incident response
b. Evidence gathering
c. Entrapment
d. Enticement

Câu 14.
Key rollover là tên gọi của quy trình nào sau đây?
a. Cấp phát khóa mới
b. Đăng ký khóa mới
c. Đăng ký gia hạn khóa để sử dụng tiếp tục sau khi khóa hết hạn
d. Tái bản khóa mới thay thế khóa cũ đã hết hạn

Câu 15.
Chứng chỉ số có các thành phần chính nào?
a. Thông tin cá nhân của người được cấp, Khoá công khai của người được cấp
b. Thông tin cá nhân của người được cấp, Khoá công khai của người được cấp, Chữ ký số của CA cấp chứng chỉ
c. Email của người được cấp, Chữ ký số của CA cấp chứng chỉ
d. Cả ba câu trên đều sai

Câu 16.
Đặc điểm nào sau đây thuộc giao thức SLIP?
a. Chỉ hỗ trợ các giao tiếp tuần tự

b. Không bảo mật
c. Hỗ trợ cho các kết nối dial-up
d. Cả ba câu trên đều đúng

Câu 17.
Hệ thống nào sau đây được cài đặt trên host cung cấp khả năng của một IDS?
a. Network sniffer
b. N-IDS
c. H-IDS
d. VPN

Câu 18.
Giao thức nào sau đây là giao thức chuẩn cho các giao tiếp trên Internet?
a. FTP
b. TCP/IP
c. HTTP
d. SMTP

Câu 19.
Loại thông tin nào sau đây không được phát hành bên ngoài công ty?
a. thông tin cá nhân
b. phân phối đầy đủ
c. thông tin cấm
d. phân phối hạn chế

Câu 20.
Phần mềm nào sau đây có khả năng ghi lại chuỗi kí tự gõ trên bàn phím của người dùng?
a. Spyware
b. Keylogger
c. Malware
d. Cả ba câu trên đều sai

Câu 21.
Con số nào sau đây thể hiện tính sẵn có cao?
a. 98%
b. 99%
c. 99.99%
d. 99.999%

Câu 22.
Mục đích cơ bản của tường lửa (firewall) là gì?
a. Hỗ trợ tìm đường giữa các nút mạng
b. Thiết lập một rào chắn giữa mạng nội bộ có độ tin cậy cao với một mạng khác có độ tin cậy thấp hơn
c. Ngăn chặn sự xâm nhập của các phần mềm độc hại
d. Tăng tốc độ kết nối cho người dùng mạng

Câu 23.
Kĩ thuật nào sau đây cho phép thiết lập một kết nối giữa hai mạng sử dụng một giao thức bảo mật?
a. Tuneling
b. VLAN
c. Internet
d. Extranet

Câu 24.
Hai người A và B sử dụng chữ ký số trong các bức điện giao dịch với nhau. Trong đó K1 là khóa mật của A, K2 là khóa mật của B, K3 là khóa công khai của A, K4 là khóa công khai của B. Nếu A nhận từ B 1 bản tin có chữ ký số thì A sẽ phải dùng khóa nào để xử lý bức điện đó?
a. K1
b. K2
c. K3
d. K4

Câu 25.
Bảo mật thông tin tập trung chủ yếu vào các mảng nào sau đây?
a. Bảo mật vật lý, bảo mật vận hành
b. Bảo mật vật lý, quản trị và chính sách, xác thực
c. Bảo mật vật lý, bảo mật vận hành, quản trị và chính sách
d. Bảo mật vật lý, bảo mật vận hành, quản trị và chính sách, xác thực

Câu 26.
Hành vi nào sau đây là một đáp ứng chủ động (active response) trong một hệ thống IDS?
a. Gửi cảnh báo đến console
b. Lãng tránh
c. Tái cấu hình router để chặn một địa chỉ IP
d. Tạo thêm một mục trong tập tin kiểm toán (audit file)

Câu 27.
Phương tiện truyền dẫn nào được phân thành 7 lớp con tùy thuộc vào hiệu suất và băng thông?
a. Cáp đồng trục
b. Cáp UTP
c. Sóng hồng ngoại
d. Cáp quang

Câu 28.
Kiểu tấn công nào mà các phần mềm IM (Instant Message) có thể gặp phải?
a. Mã độc hại (Malicious code)
b. IP spoofing
c. Tấn công kiểu Man-in-the-middle
d. Tấn công Replay

Câu 29.
Ophcrack có thể sử dụng để dò tìm password đã mã hóa ở dạng nào?
a. LM/NTLM hash
b. SHA-256
c. SHA-512
d. MD5

Câu 30.
Cấp độ bảo mật nào sau đây yêu cầu việc cho phép kiểm tra các thành phần trong hệ thống một cách độc lập, riêng lẻ?
a. EAL 4
b. EAL 5
c. EAL 6
d. EAL 7

Câu 31.
Quá trình làm cho workstation và server trở nên an toàn hơn được gọi là gì?
a. Platform hardening
b. Packet filtering
c. OS hardening
d. Firewall building

Câu 32.
Sự xác nhận của CA để bảo đảm tính chính xác và hợp lệ của một chứng chỉ số thể hiện qua yếu tố nào?
a. Khoá mật của CA cấp chứng chỉ trong chứng chỉ số đó
b. Khoá công khai của CA cấp chứng chỉ trong chứng chỉ số đó
c. Chứng chỉ gốc trong chứng chỉ số đó
d. Cả ba câu trên đều sai

Câu 33.
Phương pháp nào sau đây phân chia một mạng thành các mạng con riêng nhỏ hơn trong đó các mạng con tồn tại đồng thời trên cùng một đường dây nhưng chúng không hề biết đến các mạng con còn lại?
a. VLAN
b. NAT

c. MAC
d. Security zone

Câu 34.
Thuật ngữ Broadcasting trong mạng có nghĩa là gì?
a. Gửi một gói tin đến tất cả các máy trong mạng
b. Gửi một gói tin đến một số máy trong mạng
c. Gửi một gói tin đến một máy cụ thể trong mạng
d. Gửi một gói tin đến tất cả các máy ngoại trừ một số máy cụ thể

Câu 35.
Nhóm thành viên nào được sử dụng để quản lý truy cập mạng?
a. Nhóm an ninh
b. Nhóm truy xuất 1 lần
c. Nhóm chia sẻ tài nguyên
d. Nhóm AD

Câu 36.
Ophcrack hỗ trợ tốt cho các nền hệ điều hành nào sau đây?
a. Windows
b. Linux/Unix
c. Mac O/S
d. Web OS

Câu 37.
Hệ thống tập tin nào được sử dụng cho máy chủ Novell Netware?
a. NTFS
b. NFS
c. FAT
d. NSS

Câu 38.
Đặc điểm nào sau đây có thể bị tấn công trên các mạng không dây?
a. Phần mềm giải mã
b. IP spoofing
c. Lỗ hổng trong WAP
d. Site survey

Câu 39.
Kiểu tấn công nào xảy ra nếu một certificate hết hạn được sử dụng lặp đi lặp lại để đạt được quyền đăng nhập hệ thống?
a. Man-in-the-middle
b. Back door
c. DoS
d. Replay

Câu 40.
Chính sách nào sau đây bao gồm tất cả các khía cạnh an toàn của một tổ chức?
a. Chính sách quản trị bảo mật
b. Chính sách bảo mật thông tin
c. Chính sách bảo mật vật lý
d. Chính sách phân loại thông tin

Câu 41.
Khóa của chuẩn mật mã AES có chiều dài như thế nào?
a. 128 bit
b. 192 bit
c. 256 bit
d. Hỗ trợ cả 128, 192, 256 bit

Câu 42.
Hai người A và B sử dụng phương pháp mật mã bất đối xứng để bảo mật thông tin liên lạc với nhau. Trong đó K1 là khóa mật của A, K2 là khóa công khai của A, K3 là khóa mật của B, K4 là khóa công khai của B. Nếu A gửi cho B 1 bản tin được mật mã với khóa K4 thì B sẽ phải dùng khóa nào để giải mã?
a. K1
b. K2
c. K3
d. K4

Câu 43.
Người ta còn e ngại hành vi bên trong nào sau đây khi bảo vệ tấn công hệ thống mạng ngoài việc ngăn chặn xâm nhập từ bên ngoài?
a. Tấn công
b. Phá hoại
c. Lạm dụng
d. Cả ba câu trên đều đúng

Câu 44.
Điểm khác nhau cơ bản giữa worm và virus là gì?
a. Worm có khả năng tự nhân bản
b. Worm là chương trình độc lập, có khả năng tự lan truyền mà không cần sự hỗ trợ của chương trình khác hoặc con người
c. Khả năng phá hoại hệ thống khác nhau
d. Cả ba câu trên đều sai

Câu 45.
Thuật ngữ nào sau đây dùng để chỉ virus, worm, Trojan horse hoặc các mã tấn công?
a. Virus
b. Spam
c. Applet
d. Malware

Câu 46.
Giao thức nào sau đây được sử dụng để tạo một môi trường an toàn trong mạng không dây hiện nay?
a. WAP
b. WEP
c. WTLS
d. WPA

Câu 47.
Có bao nhiêu mục đích khi thiết kế một mô hình bảo mật?
a. 1
b. 2
c. 3
d. 4

Câu 48.
Thuật ngữ nào sau đây dùng để mô tả thông tin thô mà IDS sử dụng để phát hiện các hoạt động đáng nghi?
a. Dectection information
b. IDS Data
c. Data source
d. Sensor

Câu 49.
Giao thức SSL không có đặc điểm nào sau đây?
a. Để hiện thực SSL, cần có các thay đổi trong hệ điều hành
b. Cung cấp các chức năng về mã hóa, bảo vệ tính toàn vẹn và xác thực
c. Tương đối đơn giản và được thiết kế tốt khi so với IPSec
d. Cả ba câu trên đều đúng

Câu 50.
Lựa chọn nào sau đây thuộc nhóm phần mềm độc hại?
a. Phần mềm gián điệp (Spyware)
b. Phần mềm quảng cáo (Adware)
c. Virus máy tính
d. Cả ba câu trên đều đúng

Câu 51.
Mã hóa thay thế là phương pháp
a. Chuyển đổi hoặc trộn lẫn các chữ cái theo một cách nhất định
b. Thay đổi một ký tự hoặc biểu tượng thành một ký tự khác
c. Sử dụng thông điệp dưới dạng hình ảnh, bài báo, danh sách mua hàng, bì thư, hoặc thông điệp ẩn
d. Cả ba câu trên đều đúng

Câu 52.
Chữ kí điện tử không sử dụng với mục đích nào sau đây?
a. Xác thực người dùng
b. Bảo vệ bí mật dữ liệu
c. Chống thoái thác
d. Toàn vẹn dữ liệu

Câu 53.
Đối với việc cập nhật hệ điều hành, ta có mấy phương cách?
a. 2
b. 3
c. 4
d. 5

----------Hết----------

Sinh viên được sử dụng tài liệu, cán bộ coi thi không giải thích gì thêm