

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

Học kỳ: 2 Năm học: 2019-2020

Ngày thi: 17/7/2020 - Giờ thi: 7h

ĐỀ THI KẾT THÚC HỌC PHẦN

MÔN: An toàn bảo mật thông tin

(số câu trong đề thi: 50)

Mã đề: 222

Thời gian làm bài: 60 phút

(Sinh viên được sử dụng tài liệu, không sử dụng máy tính hoặc điện thoại)

Họ và tên : MSSV:

NỘI DUNG ĐỀ THI

Câu 1. Trong số các phương pháp định danh và xác thực sau, phương pháp nào yếu nhất?

- A. Password
- B. Token
- C. Biometrics
- D. Smart Card

Câu 2. Phương pháp MAC trong kiểm soát truy cập là viết tắt của từ nào sau đây?

- A. Most Access Control
- B. Mandatory Access Control
- C. Min Access Control
- D. Match Access Control

Câu 3. “Một hệ thống phải có chức năng lưu lại các hành động của người dùng khi thao tác trên các dữ liệu”. Chức năng này thể hiện yêu cầu nào sau đây?

- A. Bí mật (Confidentiality)
- B. Toàn vẹn (Integrity)
- C. Sẵn sàng (Availability)
- D. Chống thoái thác (Non-repudition)

Câu 4. Trong tấn công truy cập, kẻ tấn công muốn đạt được mục đích nào sau đây?

- A. Chỉnh sửa thông tin hệ thống
- B. Phá vỡ mạng máy tính và các dịch vụ của nó
- C. Truy cập vào các thông tin không được phép
- D. Cả ba câu trên đều sai

Câu 5. 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 6. Để cung cấp dịch vụ Web cho các máy trong mạng nội bộ, nhưng không để lộ thông tin của mạng nội bộ ta sẽ cài đặt Web server ở đâu

- A. Cài đặt trong intranet
- B. Cài đặt trong DMZ
- C. Cài đặt trong VLAN
- D. Cài đặt trong extranet

Câu 7. Phương pháp tấn công nào trong đó kẻ tấn công phá vỡ hệ thống bằng cách gửi số lượng lớn (hơn mức

- hệ thống có thể xử lý) các gói tin ICMP?
- A. Tấn công từ chối dịch vụ dạng ping of death
 - B. Tấn công từ chối dịch vụ dạng buffer overflow
 - C. Tấn công thoát thắc
 - D. Tấn công truy cập

Câu 8. Phương pháp xác thực nào mà ở đó server gửi client một challenge, client mã hóa và gửi ngược về server để xác thực

- A. Kerberos
- B. PAP
- C. DAC
- D. CHAP

Câu 9. Kiểu tấn công nào trong đó kẻ tấn công sẽ giả dạng là một server hợp pháp để lấy thông tin đăng nhập của người dùng?

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

Câu 10. Kiểu tấn công Smurf sử dụng giao thức nào sau đây để thực hiện quá trình tấn công?

- A. IP
- B. TCP
- C. UDP
- D. ICMP

Câu 11. Kiểu tấn công nào không cho phép người dùng hợp pháp truy xuất đến tài nguyên mạng?

- A. Worm
- B. Logic bomb
- C. DoS
- D. Social engineering

Câu 12. Loại virus nào được định kèm trong các boot sector của ổ đĩa để tránh bị phát hiện và thông báo thông tin sai về kích thước của tập tin?

- A. Trojan horse virus
- B. Stealth virus
- C. Worm
- D. Polymorphic virus

Câu 13. Người dùng A phát hiện địa chỉ IP của máy tính mình đã được sử dụng khi bắt máy tính lên. Địa chỉ IP tính được gán cho máy này, người dùng chắc chắn đã có sự cố ý trong việc gán địa chỉ IP này cho máy khác. Kiểu tấn công nào xảy ra trong trường hợp này?

- A. Man-in-the-middle
- B. Back door
- C. Worm
- D. Tấn công chặn TCP/IP

Câu 14. Nhà cung cấp chứng thực số (Certification Authorities - CAs) là gì?

- A. là công ty cung cấp các phần mềm chứng thực số cho người dùng, đóng vai trò hỗ trợ cho quá trình trao đổi thông tin an toàn
- B. là công ty cung cấp các phần mềm chứng thực số cho người dùng, xây dựng nền mô hình PKI
- C. là tổ chức phát hành các chứng thực khóa công khai cho người dùng, đóng vai trò là bên thứ ba để hỗ trợ

