Câu 1: Phòng chống tấn công Tấn công từ chối dịch vụ phân bố (DDOS)

A Chỉ có thể dùng tường lửa

B Có thể hạn chế trong bằng cách lập trình

C Hiện nay đã có cách phòng chống hiệu quả

D Cách hiệu quả duy nhất là lưu trữ và phục hồi (backup và restore)

Đáp án đúng: B

Câu 2: Bộ đệm một lần

A Khóa chỉ xài 1 lần

B Có thể không an toàn do phân phối

C Sinh khóa ngẫu nhiên

D Tất cả đều đúng

Đáp án đúng: D

Câu 3: Trong DAC, mô hình nào dung cấu trúc đồ thị tĩnh và đồ thị động

A Mô hình truy cập CSDL đa mức

B Mô hình Take-grant.

C Mô hình ma trận truy cập

Mô hình Acten (Action. Entity)

Đáp án đúng: B

Câu 4: RSA là giải thuật

A Mã công khai

B Là tên của một tổ chức quốc tế về mã hóa

C Mã khóa riêng

D Tất cả đều

Đáp án đúng: A

Câu 5: Một trong hai cách tiếp cận tấn công mã đối xứng

A Tất cả đều

B Tấn công tìm khóa

C Tấn công duyệt toàn bộ

D Tấn công tìm bản rõ

Đáp án đúng: C

Câu 6: Cơ cấu bảo mật nào sau đây được sử dụng với chuẩn không dây WAP ?

A WTLS

B SSL

C HTTPS

D Mã hóa WEP

Đáp án đúng: A

Câu 7: Phương pháp điều khiển truy cập có hiệu quả và an toàn nhất đối với mạng không dây là

A Mã hóa WEP 40 bit

B VPN

C Nhận dạng bảo mật mạng

D Mã hóa WEP 128 bit

Đáp án đúng: C

Câu 8: Bộ lọc địa chỉ MAC được định nghĩa như

A Tường lửa cá nhân

B Ngăn chặn truy cập từ một địa chỉ MAC nhất định.

C Được phép truy cập đến một địa chỉ MAC nhất định.

D Tất cả đều đúng

Đáp án đúng: D

Câu 9: Cơ cấu bảo mật mạng không dây nào sau đây là ít an toàn nhất ?

A VPN

B Mã hóa WEP 40 bit

C Bảo mật định danh mạng

D Mã hóa WEP 128 bit

Đáp án đúng: C

Câu 10: Mức mã hóa WEP nào nên được thiết lập trên một mạng 802.11b ?

A 128 bit

B 40 bit

C 28 bit

D 16 bit

Đáp án đúng: A

Câu 11: Timestamp trong message

- A Dùng để ghi nhận số lần trao đổi
- B Dùng để xác định thời gian hết hạn
- C Dùng để cho phép giao dịch
- D Tất cả đều đúng

Đáp án đúng: A

Câu 12: Tích của 2 phép thế :

- A Tương đương với 2 phép hoán vị
- B Cho ta 1 phép thế phức tạp hơn
- C Thường dung trong mã hiện đại
- D Là một phép thế

Đáp án đúng: D

Câu 13: Mã khóa công khai

- A Dùng 1 khóa để mã hóa và 1 khóa để giải mã
- B Có thể dung khóa public để mã hóa
- C A và B đều đúng
- D A và B đều

Đáp án đúng: C

Câu1 4: Trong các thư mục tấn công RSA được lưu ý, không có :

- A Tấn công tính toán thời gian
- B Tấn công toán học
- C Tấn công bản rõ
- D Tấn công brute force

Đáp án đúng: C

Câu1 5: Chỉ phát biểu . Mã đường cong elip

- A Ít tốn vùng nhớ do xử lý ít hơn RSA
- B Dung khóa công cộng và khóa riêng để tính toán khóa phiên
- C Các tính toán là tương đương

- D Độ an toàn ít hơn RSA

Đáp án đúng: D

Câu1 6: Các chuẩn giao thức mạng không dây IEEE nào sau đây là phổ biến nhất ?

- A 802.11b
- B 802.11a
- C 802.11g
- D Tất cả đều đúng

Đáp án đúng: D

Câu1 7: Các chuẩn giao thức mạng không dây nào sau đây phân phối nội dung Wireless Markup Language (WML) đến các ứng dụng Web trên các thiết bị cầm tay (PDA)?

- A WAP
- B WEP
- C 802.11g
- D SSL

Đáp án đúng: A

Câu 18: Thiết bị nào được sử dụng để cho phép các máy trạm không dây truy cập vào một mạng LAN rộng ?

- A 802.11b
- B Tường lửa
- C Điểm truy cập không dây (Wiless Access Point)
- D VPN

Đáp án đúng: D

Câu 19: Các thiết bị nào sau đây có thể sử dụng được trên mạng không dây ?

- A Máy vi tính để bàn
- B Máy tính xách tay
- C PDA
- D Tất cả các loại trên

Đáp án đúng: A

Câu 20: Kỹ thuật nào được sử dụng để bảo đảm thông tin liên lạc qua một mạng không được bảo mật ?

- A Telnet
- B SLIP
- C VPN
- D PPP

Đáp án đúng: A

Câu 21: X=Ek(Y). Bản mã là

- A Y
- B D
- C K
- D X

Đáp án đúng: D

Câu 22: Phát biểu nào là ? Hàm hash

- A Thường dung với lý do là thời gian mã hóa
- B Kết quả phụ thuộc mẫu tin
- C Thường dung để tạo chữ ký điện tử

- D Kích thước kết quả có độ dài phụ thuộc vào mẫu tin

Đáp án đúng: D

Câu 23: Trong giải thuật SHA 512, 80 từ :

- A Được tạo ra mặc định
- B Được tạo ra từ toàn bộ messenger
- C Được tạo a từ một phần của messenger
- D Tất cả đều

Đáp án đúng: B

Câu 24: Trong mô hình ma trận truy cập ,"namesalary"....

- A Time-Dependent
- B Date-Dependent
- C Context-Dependent
- D History-Dependent

Đáp án đúng: C

Câu 25: Chứng nhận chứa :

- A Chữ ký
- B Thông tin thuật toán tạo mã khoá
- C Thuật toán tạo chữ ký
- D Tất cả đều đúng

Đáp án đúng: D

Câu 26: Giao thức được sử dụng rộng rãi nhất để truy cập kiểu quay số đến một máy chủ từ xa là

- A SLIP
- B PPP
- C A và B đều đúng
- D A và B đều

Đáp án đúng: C

Câu 27: LAC (L2TP Access Control) và LNS (L2TP Network Server)) là các thành phần của giao thức đường hầm nào ?

- A IPSec
- B PPP
- C PPTP
- D L2TP

Đáp án đúng: D

Câu 28: Các giao thức nào sau đây làm việc trên lớp IP để bảo vệ thông tin IP trên mạng ?

- A IPX
- B IPSec
- C SSH
- D TACACS+

Đáp án đúng: B

Câu 29: Các giao thức xác thực nào sau đây là được sử dụng trong các mạng không dây ?

- A 802.1X
- B 802.11b
- C 802.11a
- D 803.1

Đáp án đúng: B
Câu 30: Mục đích của một máy chủ RADIUS là :

- A Packet Sniffing
- B Mã hóa
- C Xác thực
- D Thỏa thuận tốc độ kết nối

Đáp án đúng: C
Câu 31: Thám mã khi không biết khoá

- A Bài toán dễ
- B Bài toán khó
- C A & B vì phụ thuộc vào khoá
- D A & B vì phụ thuộc vào giải thuật

Đáp án đúng: B
Câu 32: Mã Ceaser của party là

- A Sduwb
- B Tduwb
- C Teuwb
- D Tất cả đều có thể phụ thuộc vào

Đáp án đúng: A
Câu 33: Phát biểu ? Kerberos

- A Đáp ứng yêu cầu không chối cãi
- B Có thể bị tấn công
- C Có thể bị tấn công Password
- D Tất cả đều

Đáp án đúng: A
Câu 34: Khoá riêng có đặc điểm

- A Khoá riêng có đặc điểm
- B Không an toàn
- C Được thay thế bằng khoá công khai
- D Thời gian thực hiện nhanh

Đáp án đúng: B
Câu 35: DAC trong DBMS có mấy mức

- A 1 mức
- B 2 mức
- C 3 mức
- D 5 mức

Đáp án đúng: B
Câu 36: Các giao thức đường hầm nào sau đây chỉ làm việc trên các mạng IP ?

- A SSH
- B IPX
- C L2TP
- D PPTP

Đáp án đúng: C
Câu 37: Tiện ích nào sau đây là một phương thức bảo mật truy cập từ xa tốt hơn telnet ?