**Ứng dụng của IPSec:**

* a. Xây dựng các website an toàn cho các ứng dụng thương mại điện tử
* b. Cho phép truy xuất từ xa một cách an toàn
* c. Xây dựng các mạng riêng ảo (VPN) trên nền Internet công cộng
* **d. Tất cả các đáp án đều đúng**

**Nguy cơ ảnh hưởng đến tính khả dụng của hệ thống thông tin:**

* a. Các tấn công từ chối dịch vụ (DoS và DDoS)
* b. Thiết bị không an toàn
* **c. Tất cả các nguy cơ trên**
* d. Virus và các loại phần mềm phá hoại khác trên máy tính

**Các bước mã hóa của chữ ký điện tử:**

* a. Chỉ sử dụng giải thuật băm để thay đổi thông điệp cần truyền đi và sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên
* b. Tất cả đều đúng
* **c. Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, Sử dụng khóa private key của người gửi để mã hóa message digest vừa thu được ở bước trên, sau đó gộp digital signature vào message ban đầu**
* d. Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu và nén dữ liệu gởi đi

**Các giao thức bảo mật thư điện tử:**

* a. Keboros, X.509
* **b. GPG, S/MIME**
* c. SHA-1, S/MINE
* d. CAST-128 / IDEA/3DES

**Các giao thức xác thực thông dụng trong hệ thống thông tin:**

* a. Tất cả đều sai
* b. CHAP
* **c. Kerberos và CHAP**
* d. Kerberos

**Phát biểu không chính xác về hệ thống xác thực TACACS+:**

* **a. Kết hợp chức năng xác thực và phân quyền**
* b. Mã hóa toàn bộ phần payload
* c. Mục đích chính việc chứng thực là xác thực quyền quản trị thiết bị
* d. Tách biệt chức năng xác thực và phân quyền

**Phương pháp tốt nhất để bảo mật dữ liệu trên đĩa cứng:**

* a. DSA
* b. SHA
* c. DES
* **d. RSA**

**Phát biểu sai về giải thuật DES:**

* a. DES dùng bộ khóa để tạo ra các khóa con dùng cho mỗi vòng (chu trình mạng Feistel), các khóa con có chiều dài là 48 bits
* **b. DES được xem là an toàn hơn 3DES do sử dụng khóa có chiều dài 64 bits**
* c. Dữ liệu được mã hóa trong các khối dữ liệu chiều dài 64 bits
* d. DES sử dụng khóa có chiều dài 64 bits

**Phát biểu không chính xác về Rootkit:**

* a. Máy bị Rootkit được coi là bị chiếm quyền root
* b. Rootkit được xếp vào nhóm các phần mềm Trojan
* **c. Những công cụ thông dụng của hệ điều hành có thể phát hiện được Rootkit**
* d. Rootkit thường gồm nhiều Backdoor giúp xâm nhập vào hệ thống dễ dàng hơn ở lần sau
* e. Rootkit là bộ công cụ dùng để che giấu sự tồn tại của file hay tiến trình dù nó vẫn hoạt động

**Giải thuật không phải nhóm giải thuật băm:**

* a. SHA-1
* **b. DES**
* c. HMAC
* d. MD5

**Phát biểu đúng về tính năng của BPDU Guard:**

* **a. BPDU Guard là một tính năng có thể giúp ngăn chặn các switch giả mạo và giả mạo trên các cổng truy cập**
* b. Tất cả các đáp án trên đều đúng
* c. Tính năng học nhanh các địa chỉ MAC address
* d. Tính năng xây dựng STP trên Switch (spanning-tree)
* e. Tính năng tạo ra danh sách địa chỉ MAC address cho phép truy cập trên Switch

**Cổng được HTTPS sử dụng:**

* a. 80
* b. 8080
* **c. 443**
* d. 21
* e. 53

**VPN là viết tắt của:**

* **a. Virtual Private Network**
* b. Virtual Perimeter Network
* c. Virtual Public Network
* d. Virtual Protocol Network

**Biện pháp không phải bảo mật mạng không dây:**

* a. Mã hóa WEP
* b. Mã hóa WPA2
* c. Mã hóa WPA
* **d. VPN**

**Tính năng của câu lệnh storm control:**

* a. Giới hạn gói tin broadcast là 50 bit trên giây
* **b. Giới hạn phần trăm gói tín broadcast là 50**
* c. Giới hạn gói tin broadcast là 50 gói trên giây
* d. Tối đa có 50 gói tín broadcast

**Lợi ích chính của VPN:**

* a. Hiệu suất mạng tốt hơn
* b. Ít bị lỗi hơn
* c. Cải thiện an ninh
* **d. Giảm chi phí**

**Phát biểu đúng về tính năng của câu lệnh spanning-tree portfast:**

* a. Tất cả các đáp án đều đúng
* **b. PortFast được cấu hình trên các cổng truy cập (access) kết nối với một máy trạm hoặc máy chủ để cho phép chúng hoạt động nhanh hơn**
* c. PortFast được cấu hình trên các cổng trunk kết nối hai router với nhau
* d. PortFast được cấu hình trên các cổng trunk kết nối hai switch với nhau

**Phát biểu đúng về chức tính năng Root Guard:**

* a. Không đáp án nào đúng
* b. A
* c. B
* **d. A và B**

**Giải thuật SHA-1 dùng để:**

* a. Tạo khóa đối xứng
* **b. Tạo một giá trị băm có độ dài cố định 160 bit**
* c. Tạo chữ ký số
* d. Tạo một giá trị băm có độ dài cố định 256 bit

**Loại tấn công nhắm vào cơ sở dữ liệu SQL:**

* a. Cross-site scripting
* b. XML injection
* **c. SQL injection**
* d. Buffer overflow

**Thứ tự có hệ số bảo mật từ cao đến thấp khi cấu hình các lớp mạng:**

* a. LAN, Internet, DMZ
* b. DMZ, Internet, LAN
* **c. DMZ, LAN, Internet**
* d. LAN, DMZ, Internet

**Thành phần không nằm trong mô hình an ninh mạng AAA:**

* **a. Availability**
* b. Accounting
* c. Authorization
* d. Authentication

**Giải thuật MD5 dùng để:**

* **a. Kiểm tra tính toàn vẹn dữ liệu**
* b. Bảo mật một thông điệp
* c. Phân phối khóa mật mã
* d. Xác thực một thông điệp

**Phát biểu đúng về kỹ thuật tấn công sử dụng lại (Replay):**

* a. Hacker cài đặt vào máy nạn nhân để có thể truy cập vào trong thời gian sau cho dù lần xâm nhập trước đó đã bị phát hiện ra
* b. Hacker sẽ chặn các gói dữ liệu gửi đi giữa 2 host, thay thế bằng những gói dữ liệu khác và gửi chúng đi
* c. Hacker sẽ tìm cách nắm quyền điều khiển một giao dịch đang diễn ra và loại bỏ truy cập từ người dùng hợp pháp
* **d. Hacker sẽ dùng 1 kỹ thuật tấn công (như nghe lén) để lấy được các thông tin quan trọng (chẳng hạn như username và password), ghi nhận và lưu trữ lại để có thể dùng cho tấn công sau này**

**Mục đích của một máy chủ RADIUS:**

* a. Mã hóa
* b. Packet sniffing
* **c. Xác thực**
* d. Thỏa thuận tốc độ nối kết