# CÂU HỎI THAM KHẢO

**Câu 1.** Trong an toàn mạng, phát biểu nào là SAI về giải thuật băm?

a. Giải thuật băm MD5 có giá trị đầu ra là 1 số có độ dài 128 bits
b. Giải thuật SHA-1 có tính bảo mật cao hơn MD5
c. Giải thuật băm không dùng để mã hóa dữ liệu mà dùng để mã hóa khóa bí mật
d. Kết quả của giải thuật băm là 1 số (digest) có độ dài cố định và được gửi đi kèm với dữ liệu

**Câu 2.** Ý tưởng nào dùng để thiết lập các đường hầm (tunnel) trong mạng VPN?

a. Chứng thực 2 chiều trên đường truyền
b. Bao gói dữ liệu gốc bên trong gói dữ liệu đã được mã hóa
c. Phân quyền chi tiết cho từng người dùng cụ thể
d. Nén dữ liệu

**Câu 3.** Để ngăn ngừa tấn công giả mạo trên giao diện của switch dùng giải thuật STP, câu lệnh nào bên dưới dùng trên switch SW-A là đúng?

a. SW-A(config-if)# spanning-tree bpduguard enable
b. SW-A(config-if)# spanning-tree bpduguard on
c. SW-A(config-if)# switchport port-security
d. Tất cả các câu trên đều đúng

**Câu 4.** Các nguy cơ nào sau đây có thể ảnh hưởng đến tính khả dụng của hệ thống thông tin?

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

**Câu 5.** Tính bảo mật (Confidentiality) trong an toàn mạng đề cập đến điều gì?

a. Đảm bảo thông tin không bị thay đổi trái phép
b. Ngăn chặn truy cập trái phép vào dữ liệu
c. Đảm bảo hệ thống luôn sẵn sàng khi cần thiết
d. Ngăn chặn các cuộc tấn công từ chối dịch vụ (DDoS)

**Câu 6.** Điều nào sau đây thể hiện tính toàn vẹn (Integrity) trong an toàn mạng?

a. Dữ liệu không bị sửa đổi trái phép trong quá trình lưu trữ và truyền tải
b. Người dùng không thể truy cập dữ liệu mà không có quyền
c. Hệ thống vẫn hoạt động ngay cả khi có lỗi phần cứng
d. Ngăn chặn các cuộc tấn công phishing (lừa đảo)

**Câu 7.** Đối với giải thuật DES, trong các phát biểu sau phát biểu nào là sai?

a. Dữ liệu được mã hóa trong các khối dữ liệu chiều dài 64 bits
b. DES được xem là an toàn hơn 3DES do sử dụng khóa có chiều dài 64 bits.
c. 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.
d. DES sử dụng khóa có chiều dài 64 bits

**Câu 8.** Giải thuật nào bên dưới không phải nhóm giải thuật băm?

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

**Câu 9.** Lý do chính để sử dụng VPN là gì?

a. Tăng độ an toàn cho đường truyền Internet
b. Giảm chi phí khi cần thiết lập đường kết nối an toàn giữa 2 vị trí ở cách xa
c. Tăng tốc độ cho đường truyền Internet
d. Đường thuê bao leased-line kết nối trực tiếp 2 vị trí xa nhau không an toàn

**Câu 10.** Firewall loại nào cho phép duyệt sâu gói tin, cho phép firewall kiểm tra trên tất cả các tầng?

a. Cisco ASA Firewall
b. Cisco PIX Firewall
c. NGFW (Next-Generation Firewall)
d. Tất cả các đáp án đều đúng.

**Câu 11.** Hãy chọn phát biểu đúng nhất về nguyên lý hoạt động của IDS?

a. Duy trì một cơ sở dữ liệu về các dấu hiệu tấn công (signature database).
b. Phân tích các gói dữ liệu lưu thông trên mạng để tìm dấu hiện của tấn công.
c. Phân tích các dữ liệu trong nhật ký hệ thống (system log) để phát hiện dấu hiệu của tấn công.
d. Tất cả các đáp án đều đúng

**Câu 12.** Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là gì?

a. IPS phát hiện xâm nhập hiệu quả hơn
b. IPS có khả năng chủ động ngăn chặn xâm nhập
c. IDS phát hiện xâm nhập hiệu quả hơn
d. IDS có khả năng chủ động ngăn chặn xâm nhập

**Câu 13.** Chọn phát biểu đúng về tính năng của câu lệnh spanning-tree portfast trên thiết bị Switch.

a. 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.
b. PortFast được cấu hình trên các cổng trunk kết nối hai switch với nhau
c. PortFast được cấu hình trên các cổng trunk kết nối hai router với nhau
d. Tất cả các đáp án đều đúng

**Câu 14.** Bộ qui tắc được các thiết bị phát hiện/ngăn ngừa xâm nhập mạng (IDS/ÍP) dựa vào để phát hiện các xâm nhập điển hình được gọi là gì?

a. Rules b. Attack rules c. Signatures d.Logfile