CÂU HỎI CHƯƠNG VIII
Môn: MẬT MÃ VÀ AN NINH MẠNG
-o0o-

I. Câu hỏi

1. Cho biết ba loại thâm nhập bất hợp pháp.
2. Ba lợi ích có thể được cung cấp bởi một hệ thống phát hiện xâm nhập là gì?
3. Phân biệt hai hướng tiếp cận để phát hiện thâm nhập bất hợp pháp.
4. Phân biệt hai hệ thống phát hiện thâm nhập bất hợp pháp.
5. Cho biết các vấn đề nảy sinh đối với các hệ thống ngăn chặn bất hợp pháp (IPS).

II. Câu hỏi trắc nghiệm

1. Hướng phát hiện thâm nhập bất hợp pháp nào liên quan đến việc thu thập hành vi người dùng hợp pháp trong một khoảng thời gian và sau đó phân tích đánh giá:

a. Phát hiện dựa trên thống kê
b. Phát hiện dựa trên quy tắc
c. Lai tạo
d. Các câu trên đều sai

2. Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:

a. Để xây dựng hệ thống phát hiện thâm nhập bất hợp pháp ta có hai hướng tiếp cận là rule-based detection và behavior-based detection.
b. Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại.
c. Một hệ thống phát hiện thâm nhập bất hợp pháp hiệu quả có thể kết hợp với bức tường lửa để ngăn chặn ngay các xâm nhập.
d. Nó cho phép ta thu thập thông tin về các kỹ thuật xâm nhập đã được sử dụng để tăng cường cho công tác phòng chống xâm nhập.

3. Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?

a. Chọn đáp ứng thích hợp
b. Xét các ngưỡng
c. Hiện thực chính sách
d. Chọn thành phần, hệ thống để theo dõi

4. Nếu một tổ chức muốn bảo vệ một máy chủ tránh bị người dùng hợp pháp phá hoại, hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?

a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

5. Nếu một tổ chức muốn phát hiện các tấn công với chi phí thấp thì hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?

a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai