CHƯƠNG 1

1.Đâu là thành phần trong An ninh mạng? (chọn nhiều câu trả lời)

(0.5 Points)

Tường lửa

Điều khiển truy cập

Bảo mật dữ liệu truyền

An toàn ứng dụng/ dịch vụ

Ngăn chặn tấn công xâm nhập

2.Những sự kiện có khả năng ảnh hưởng đến an toàn của hệ thống được gọi là:

(0.5 Points)

Rủi ro

Nguy cơ

Điểm yếu

Lỗ hổng

3.Theo bạn, đưa USB với các files cá nhân vào hệ thống có gây nguy cơ mất an toàn thông tin cho người dùng không?

(0.5 Points)

Có

Không

4.Tính bí mật trong HTTT có thể gồm (chọn nhiều câu trả lời)

(0.5 Points)

Các thông tin liên quan đến An ninh quốc gia

Dữ liệu tài nguyên trên internet

Các thông tin cá nhân

Các thông tin mang tính sỡ hữu trí tuệ của doanh nghiệp

5.Các đe dọa/ nguy cơ với vùng hệ thống ứng dụng

(0.5 Points)

Truy cập được phép đến trung tâm dữ liệu

Các vấn đề hỏng hóc và mất dữ liệu

Tấn công kiểu vét cạn vào tên người dùng

Thăm dò và rò quét các cổng dịch vụ

6.Hầu hết dữ liệu được truyền dưới dạng rõ (plaintext) là nguy cơ ở vùng hạ tầng thông tin nào?

(0.5 Points)

LAN

LAN to WAN

WAN

Truy cập từ xa

7.Theo bạn, hình thức tấn công nào thu thập tài khoản mật khẩu, giúp hacker kiểm soát, điều khiển máy tính, phá hoại dữ liệu nạn nhân từ xa ?

(0.5 Points)

Mã độc

Lừa đảo trực tuyến

Từ chối SQL

Lừa đảo mạng ATM

8.Lĩnh vực nào không có trong An toàn Thông tin?

(0.5 Points)

An toàn máy tính

Đảm bảo thông tin

Kết nối thông tin

9."Tường lửa, mạng VPN" nằm trong lớp phòng vệ nào?

(0.5 Points)

Lớp an ninh tổ chức

Lớp an ninh mạng

Lớp an ninh hệ thống

10.Bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại được gọi là:

(0.5 Points)

Điểm yếu

Nguy cơ

Lỗ hổng

11.Các đe dọa đối với vùng máy trạm?

(0.5 Points)

Truy cập trái phép vào máy trạm

Tấn công phá hoại từ các nhân viên bất mãn

Truy cập trái phép vào hệ thống dữ liệu

Các lỗ hổng an ninh trong hệ điều hành máy chủ

Người dùng tải các tập tin trái phép

12.An toàn HTTT là việc đảm bảo các thuộc tính an ninh an toàn nào của HTTT?

(0.5 Points)

Bí mật, sẵn dùng, toàn vẹn

Bí mật, đảm bảo, sẵn dùng

Bí mật, toàn vẹn, đảm bảo

13.Các cơ chế nào đảm bảo sự toàn vẹn của thông tin?

(0.5 Points)

Cơ chế ngăn chặn

Cơ chế hồi phục

Cơ chế phát hiện

Cơ chế thành lập

14.Các đe dọa/ nguy cơ đối với vùng LAN

(0.5 Points)

Truy nhập trái phép vào mạng LAN vật lý

Thăm dò và rà quét trái phép các cổng dịch vụ

Hầu hết dữ liệu được truyền dưới dạng plantext

Tấn công DoS và DDoS

15.Tính toàn vẹn của HTTT bị phá vỡ khi: (chọn nhiều câu trả lời)

(0.5 Points)

Chặn đứng và thay đổi gói tin được gửi qua internet

Chỉnh sửa các file được lưu trữ trên máy tính khi được phép

Sự cố đường truyền dẫn đến thông tin bị sai lệch

Thay đổi giao diện trang chủ của một website

16.Sự bí mật của thông tin phải được xem xét dưới dạng 2 yếu tố tách rời nào?

(0.5 Points)

Sự chuyển đổi của thông tin và nội dung của thông tin đó

Sự tồn tại của thông tin và nội dung của thông tin đó

Sự tồn tại và chuyển đổi của thông tin đó

17.Tính toàn vẹn được xét trên 2 khía cạnh nào?

(0.5 Points)

Nguồn gốc và chức năng

Chức năng và nội dung

Nội dung và nguồn gốc

18.Điểm yếu của an toàn thông tin có thể tồn tại ở đâu trong hệ thống?

(0.5 Points)

Phần cứng

Phần mềm

Cả 2 phần trên

19.Nguyên tắc đảm bảo an toàn thông tin:

(0.5 Points)

Một lớp, một công cụ phòng vệ riêng rẽ vẫn đảm bảo an toàn

Phòng vệ nhiều lớp không có chiều sâu

Cân bằng giữa tính chi phí, hữu dụng và an toàn

Tồn tại HTTT an toàn tuyệt đối

20.Tỉ lệ phục vụ trong tính sẵn dùng của HTTT được tính bằng:

(0.5 Points)

(Uptime)/(Uptime - Downtime)

(Uptime)/(Uptime + Downtime)

(Downtime)/(Uptime + Downtime)

(Uptime)/(Uptime × Downtime)