**ATTT - GK**

**(private)**

**Note : Ai có đáp án khác thì ghi đỏ dưới câu đó để, để mn còn biết mà vào thảo luận xem có đúng ko .**

1. **Tính toàn vẹn của hệ thống thông tin là đặc tính của hệ thống mà trong đó:**

a. Thông tin không bị sửa đổi hoặc xóa bỏ bởi người sử dụng.

b. Thông tin không bị thay đổi theo thời gian.

c. Thông tin không bị truy xuất bởi những người không được phép.

d. **Thông tin không bị thay đổi, hư hỏng hay mất mát.**

1. **Kỹ thuật tấn công nào sau đây liên quan đến giao thức IP:**

a. Mã nguồn độc hại.

**b. Giả mạo IP.**

c. Tấn công dạng "Man in the middle”.

d. Tấn công chuyển tiếp.

1. **Liệt kê các mục tiêu của an toàn hệ thống theo thứ tự ưu tiên giảm dần:**

**a. Ngăn chặn, phát hiện, phục hồi.**

b. Phát hiện, ngăn chặn, phục hồi.

c. Phát hiện và ngăn chặn.

d. Phát hiện và phục hồi.

1. **Kỹ thuật tấn công nào sau đây không dựa trên giao thức TCP/IP:**

a. SYN/ACK flooding.

b. TCP sequence number attack.

c. ICMP attack.

**d. Software exploitation.**

1. **Kỹ thuật tấn công nào sau thực hiện chèn vào các website động những đoạn mà script nguy hiểm:**

**a. XSS.**

b. Css.

c. SQL Injection.

d. Dos.

1. **Chương trình sniffer có thể bắt được thông tin trao đổi trên mạng là dựa vào nguyên tắc:**

**a. broadcast**

b. unicast

c. multicast

d. anycast

1. **Giai đoạn nào sau đây của một cuộc tấn công dùng để thực hiện leo thang đặc quyền?**

a. Reconnaissance

b. Scanning

**c. Gaining Access**

d. Maintaining Access

1. **Máy chủ Web của một công ty được cấu hình những dịch vụ sau: HTTPS, FTP, SMTP. Máy chủ này được đặt trong vùng DMZ. Các cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này là:**

a. 119, 21, 80, 23

b. 434, 80, 25, 20

**c. 20, 21, 25, 443**

d. 110, 443, 21, 59

1. **Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm hệ điều hành?**

**a. Cài đặt bản service pack mới nhất**

b. Cài đặt lại hệ điều hành thông dụng

c. Sao lưu hệ thống thường xuyên

d. Shutdown hệ thống khi không sử dụng

1. **Điều gì xảy ra khi máy X sử dụng kĩ thuật ARP Spoofing để nghe lén thông tin từ máy Y?**

**a. X giả mạo địa chỉ MAC của Y**

b. X giả mạo địa chỉ IP của Y

c. Y giả mạo địa chỉ MAC của X

d. Y giả mạo địa chỉ IP của X

1. **Kỹ thuật tấn công nào sau dựa vào giao thức ICMP:**

a. Man in the middle

b. Rogue

**c. Ping of the death**

d. SYN flood

1. **Các điểm yếu an ninh có thể xảy ra trong một hệ thống mạng là:**

a. Đường truyền (cáp đồng, cáp quang,...)

b. Chính sách an ninh (quy định, quy trình vận hành,...)

c. Thiết bị mạng (Firewall, Router,...)

**d. Tất cả**

1. **Authentication là thuật ngữ dùng để chỉ cơ chế:**

**a. Xác thực người dùng khi đăng nhập vào hệ thống**

b. Phân quyền người dùng khi họ đăng nhập thành công

c. Theo dõi người dùng trong quá trình log on và log off

d. Tất cả đều sai

1. **Để đảm bảo an toàn thông tin cho một hệ thống, có thể sử dụng giải pháp:**

a. Mã hóa dữ liệu và đường truyền

b. Tường lửa bảo vệ hệ thống mạng

c. Phân quyền truy cập thông tin

**d. Kết hợp các biện pháp trên**

1. **Quá trình kết thúc kết nối theo giao thức TCP sử dụng các cờ nào sau:**

**a. ACK**

b. SYN

**c. FIN**

d. RST

e. PSH

1. **Đặc trưng của các chương trình mã độc Trojan là:**

a. Chỉ hoạt động trên hệ điều hành Windows

**b. Không có khả năng tự lây lan**

c. Phát tán qua email

d. Phát tán qua lỗ hổng phần mềm

1. **Để phát hiện một máy tính hiện đang bị tấn công, điều khiển từ xa hay không, người ta có thể dùng những cách nào:**

a. Kiểm tra kết nối trên máy tính

b. Quét cổng

c. Phân tích dữ liệu mạng

**d. Tất cả các cách trên**

1. **Chọn phát biểu đúng về mã khóa công khai:**

**a. Dùng một khóa để mã hóa dữ liệu, một khóa để giải mã**

b. Chỉ cần dùng một khóa có thể mã hóa và giải mã dữ liệu

c. Người ta sử dụng public key để giải mã dữ liệu

d. Tất cả đều không đúng

1. **Mã độc Botnet thường sử dụng để thực hiện hình thức tấn công nào sau đây:**

**a. DDoS**

b. DoS

c. Relay Attack

d. Jamming Attack

1. **Các cơ chế bảo vệ tính bí mật của thông tin:**

a. Mật mã hoá toàn bộ thông tin trong hệ thống

b. Xây dựng các cơ chế điều khiển truy xuất (access control) phù hợp

c. Lắp đặt các phương tiện bảo vệ hệ thống thông tin ở mức vật lý

**d. Tất cả các cơ chế trên**

1. **Ngôn ngữ lập trình chủ yếu sử dụng trong Metasploit là:**

a. Java

b. Python

**c. Ruby**

d. C++

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

a. Thiết bị không an toàn

b. Các tấn công từ chối dịch vụ (DoS và DDoS)

c. Virus và các loại phần mềm phá hoại khác trên máy tính

**d. Tất cả các nguy cơ trên**

1. **Kỹ thuật tấn công nào sau đây khai thác phiên kết nối giữa các máy tính:**

a. SQL Injection

b. DoS

**c. Session Hijacking**

d. System Hacking

1. **Phương thức truy cập từ xa nào sau đây có tính bảo mật cao:**

a. SSL

**b. SSH**

c. IPSec

d. VPN

1. **Authorization là thuật ngữ dùng để chỉ cơ chế:**

a. Xác thực người dùng khi đăng nhập vào hệ thống

**b. Phân quyền người dùng khi họ đăng nhập thành công**

c. Theo dõi người dùng trong quá trình log on và log off

d. Tất cả đều sai

1. **Bộ lọc địa chỉ MAC trong các router wi-fi:**

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

b. Cho phép truy cập từ một địa chỉ IP nhất định

c. Chỉ có thể ngăn chặn truy cập chứ không thể cấp phép truy cập theo địa chỉ MAC

d. Hoạt động hiệu quả nhưng cần phải cấu hình kèm địa chỉ IP bị chặn

1. **Chức năng nào sau đây không phải là của một phần mềm giám sát an ninh mạng:**

a. Theo dõi hệ thống theo thời gian thực

b. Phát hiện mã chương trình có hại trước khi được thực thi

c. Theo dõi tham số hệ thống

**d. Chia sẻ dữ liệu và phân quyền sử dụng**

1. **Tấn công Social Engineering nhằm lợi dụng sơ hở của:**

a. Email

b. Local Area Network

**c. Người dùng**

d. Peer to Peer Network

1. **Quá trình thu thập thông tin trên một máy đích được gọi là:**

a. DoS

b. SQL Injection

c. Scanning

**d. Foot Printing**

1. **Kỹ thuật tấn công sniffer có thể lấy thông tin username và password khi NSD dùng giao thức:**

a. SSH (Secure Shell)

b. SSL (Secure Sockets Layer)

**c. FTP (File Transfer Protocol)**

d. HTTPS (Hypertext Transfer Protocol qua SSL)

1. **Tấn công SQL Injection cho phép kẻ tấn công:**

**a. Lợi dụng lỗ hổng trong kiểm tra dữ liệu nhập vào các ứng dụng**

b. Lợi dụng cống của dịch vụ

c. Lợi dụng cơ chế Sniffer

d. Lợi dụng kỹ thuật Man in The Middle

1. **Quá trình bắt tay 3 bước theo giao thức TCP sử dụng các cờ nào sau:**

**a. ACK**

**b. SYN**

c. FIN

d. RST

e. PSH

f. URG

g. Không sử dụng cờ nào

1. **Kỹ thuật tấn công nào sau đây không dựa vào cơ chế của TCP/IP?**

a. SYN/ACK flooding

b. TCP sequence number attack

c. ICMP attack

**d. Ransomware**

1. **Để khai thác lỗ hổng bảo mật, người ta thường:**

a. Tấn công quét mật khẩu

b. Kiểm thử bảo mật

**c. Sử dụng các công cụ thăm dò, phát hiện**

d. Lập trình truy xuất từ xa

1. **Công cụ nào sau đây cho phép theo dõi các kết nối trong thời gian thực?**

a. Netstat

b. Fport

**c. TcpView**

d. Ettercap

1. **Giao thức nào sau đây có chức năng bảo mật gói tin IP trên mạng?**

**a. IPSec**

b. IPX

c. SSH

d. TACACS+

1. **Giao thức nào được dùng để mã hóa dữ liệu trao đổi giữa Client và Server theo mô hình TCP/IP?**

a. FTP

b. HTTP

**c. SSL**

d. IMAP

1. **Phân tích dữ liệu trên mạng không được sử dụng để:**

**a. Lưu trữ dữ liệu**

b. Phát hiện các sự cố về mạng

c. Tìm hiểu các giao thức mạng

d. Báo cáo, thống kê về trạng thái của mạng

1. **Trong an toàn thông tin, thuật ngữ IDS dùng để chỉ?**

**a. Hệ thống phát hiện xâm nhập**

b. Hệ thống tường lửa

c. Hệ thống phân tích mã độc

d. Hệ thống tối ưu hiệu suất máy chủ RADIUS

1. **Virus máy tính là một phần mềm:**

a. Do lỗ hổng của website tạo ra

b. Do lỗ hổng của Windows tạo ra

**c. Do con người viết ra nhằm phục vụ cho các mục đích phá hoại**

d. Được tạo ra ngoài ý muốn do lỗi lập trình của người viết.

1. **Làm thế nào để ngăn chặn lỗ hổng máy chủ?**

a. Thay đổi mật khẩu

**b. Tăng cường bảo mật hệ thống**

c. Hạn chế thông tin đăng nhập

d. Sử dụng dịch vụ công cộng

1. **Kỹ thuật Brute force attack sử dụng cách nào sau:**

a. Tấn công từ chối dịch vụ

b. Tấn công mạng không dây

**c. Thử mật khẩu bằng cách liệt kê các giá trị có thể được**

d. Khai thác thông tin người dùng

1. **Công dụng chính của Metasploit là gì trong lĩnh vực an ninh mạng?**

a. Phân tích dữ liệu

b. Quản lý cơ sở dữ liệu

**c. Kiểm thử bảo mật và khai thác lỗ hổng**

d. Tạo ứng dụng di động

1. **Câu lệnh: union select 1, group\_concat(column\_name), 3, 4, 5, 6 from information\_schema.columns where table\_name= CHAR(97, 100, 109, 105, 110) dùng để truy vấn trị:**

**a. admin**

b. user

c. sinhvien

d. table

1. **Công cụ nào có thể dùng để xem tất cả các kết nối mạng đang có trên máy tính:**

**a. netstat**

b. ipconfig

c. ping

d. tracert

1. **Công cụ nào sau dùng để bắt gói tin trên mạng:**

**a. Wireshark**

b. Nmap

c. Cain&Abel

d. Havij

1. **Một thông điệp "ABC" được gửi đi trên mạng, nhưng bên nhận nhận được thông điệp có nội dung không đúng như thông điệp gốc. Tính chất nào sau đây đã không được đảm bảo trong quá trình truyền thông điệp này:**

a. Tính bí mật

b. Tính sẵn sàng

**c. Tính toàn vẹn**

d. Tính bí mật và tính toàn vẹn

1. **Để chuyển từ địa chỉ private IP sang public IP, người ta sử dụng cơ chế nào sau:**

**a. NAT**

b. VPN

c. IPSec

d. VLAN

1. **Mục đích chính của tấn công từ chối dịch vụ DoS (Denial of Service) là:**

a. Phá hoại Database

**b. Ngăn chặn khả năng sẵn sàng cung cấp dịch vụ của Server**

c. Thu thập thông tin của đối tượng tấn công

d. Tất cả đều sai