**Đề thi giữa kì HK1 năm học 2023- 2024**

**Môn: Thực tập An ninh máy tính**

**Thời gian: 60 phút**

**Điểm:**

**Họ tên Sinh viên: Trần Như Nguyện Mã số Sinh Viên: DH52007186**

**Lớp: D20\_TH10**

**Lưu ý:**

* **Làm bài trực tiếp trên bài thi, chụp hình bài làm dán vào bài thi.**
  + **Trả lời câu trả lời chi tiết**
  + **Chụp hình rõ ràng, toàn màn hình, thấy họ tên sinh viên**
  + **Máy kali có họ tên đúng với họ tên sinh viên**
* **Nghiêm cấm copy bài, copy bài bị 0đ cả hai.**
* **Được sử dụng tài liệu.**
* **Link nộp bài trên drive:**

[**https://drive.google.com/drive/folders/1BVr9hhJpXwd3KKlZxE0qebH4rL7javTf?usp=sharing**](https://drive.google.com/drive/folders/1BVr9hhJpXwd3KKlZxE0qebH4rL7javTf?usp=sharing)

**Yêu Cầu:**

**Câu 1: Thực hành Reconnaisance (2 điểm)**

* Hãy sử dụng các kỹ thuật trong footprinting và enumeration hãy thăm dò địa chỉ 119.82.135.103 address (dùng hostname recon, geo-recon, recon-ng, Netcraft, Dnsenum, Idserve, ping, nslookup,…):
  + Cho biết tên miền tương ứng địa chỉ (0.5đ)  
    A computer screen shot of a computer error

    Description automatically generated
  + Cho biết địa chỉ thuộc tổ chức nào (0.5đ)



* + Cho biết vị trí địa lý của địa chỉ đó (0.5đ)

A computer screen shot of a computer

Description automatically generated

* + Cho biết thông tin máy chủ đang sử dụng địa chỉ đó (chạy ứng dụng, port gì) (0.5đ)  
    A screenshot of a computer

    Description automatically generated

**Câu 2: Phân tích lỗ hổng (6 điểm)**

Câu 1: Hãy tìm kiếm máy chủ thi, cho biết IP Address, địa chỉ MAC và hostname máy chủ? (1đ)  


Câu 2: (2đ)

1. Máy chủ thi mở các port và dịch vụ tương ứng nào, tên Workgroup? (1đ)  
   A computer screen shot of a computer

   Description automatically generated
2. Cho biết Phiên bản của hệ điều hành và phiên bản các dịch vụ tương ứng của máy chủ thi? (1đ)  
   A computer screen shot of a program

   Description automatically generated  
   A computer screen shot of a program

   Description automatically generated

Câu 3: Hãy cho biết firewall máy chủ thi đang tắt hay mở? (1đ) A computer screen with white text

Description automatically generated

Câu 4: Dùng Nessus kiểm tra máy chủ thi có bao nhiêu lỗ hổng bảo mật? Cho biết kết quả về các mức độ lỗ hổng? (2.0đ)  
A screenshot of a computer

Description automatically generated

**Câu 3: Giải pháp phòng chống (2 điểm)**

Câu 1: Từ kết quả câu 2 cho biết các loại lỗ hổng nguy hiểm và khả năng khai thác lỗ hổng đó? (0.5đ)

Câu 2: Đưa ra hướng khắc phục các lỗ hổng để hệ thống an toàn? (1.5đ)   
bật firewall của máy  
update windown thường xuyên  
đặt lại mật khẩu 6 tháng một lần trên 10 kí tự  
mk bao gồm kí tụ in hoa , chữ thường , kí tự đặt biệt.

**Trả lời:**