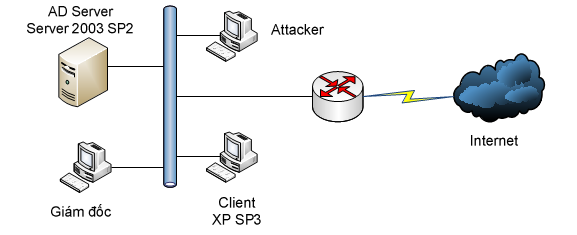
PRACTICE:

PHÂN TÍCH ĐÁNH GIÁ AN TOÀN MẠNG

Ta có sơ đồ mạng sau

  
**Mô tả sơ đồ mạng:**- Cấu hình Window Server 2003 làm các chức năng sau cho  
o DHCP Server  
o DNS Server  
o Acitve Directory Server  
o IIS Server version 7.0 (web server)  
- Các client trong mạng điều là thành viên bên trong domain.  
- Một máy client sử dụng window xp sp3 . Trên máy XP SP 3 có các user :  
client 1, client 2, client 3, và user admin , có quyền quản lý toàn bộ hệ thống. Trong 3 user client trên, có 2 user đặt password ít hơn 7 ký tự (4 ký tự) và 1 client đặt passowrd nhiều hơn 7 ký tự  
- Giả sử bạn là 1 user thường (attacker) chung một mạng LAN như sơ đồ trên.  
**Yêu cầu :  
Phần 1 : Phát hiện lổ hổng trong mạng  
Câu 1: Sinh viên thực hiện**1.1 Cài đặt chương trình scan để xác định IP của máy Client SP3, Server 2003, Giám đốc   
1.2 Cài đặt Nmap trên máy đóng vai trò attacker   
1.3 Cài đặt Nessus trên máy đóng vai trò attacker   
**Câu 2 : Xác định các dịch vụ**

2.1 Xác định phiên bản hệ điều hành các máy trong mạng  
2.2 Xác định các port đang mở trên máy tính theo nhiều cách  
2.3 Xác định các dịch vụ tương ứng với các port   
**Câu 3 : Sử dụng Nmap và Nessus để scan các vulnerability (lổ hổng) trên máy client xp** sp3.  
3.1 Sử dụng Script Engine của Nmap để scan lỗi hệ điều hành

3.2 Sử dụng Nessus để scan lỗi   
3.3 Xác định lỗi cho phép từ xa truy cập và thực thi trái phép vào máy XP SP3