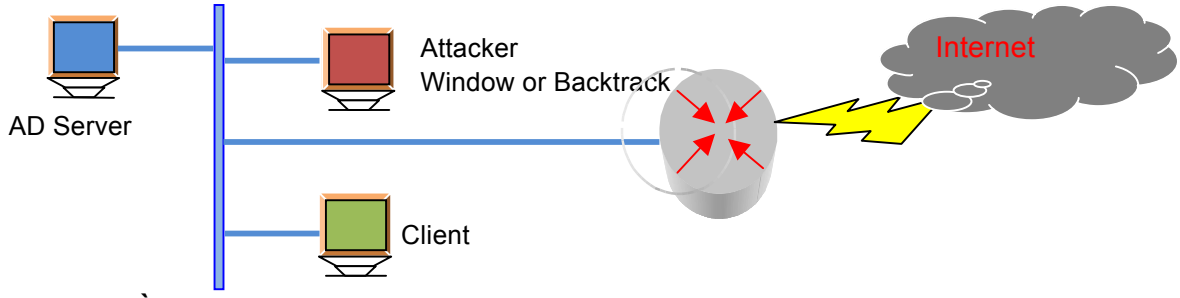
**Bài thực hành số 2: Quét mạng (Scanning Networks)**

| **Nội dung yêu cầu: Xác định các lỗ hổng bảo mật và cách khắc phục** |
|---|

**Ta có sơ đồ mạng sau:**




**Mô tả sơ đồ :**

| AD server | Client | Attacker |
|---|---|---|
| **192.168.x.2/24** | **192.168.x.3/24** | **192.168.x.4/24** |

1. Cấu hình win server làm các chức năng sau:
   a. DHCP Server
   b. DNS Server
   c. Active Directory Server
   d. IIS
2. Các client trong mạng đều là thành viên thuộc domain.
3. Một máy Client có 3 user: client 1, client 2, client 3, và user admin có quyền quản lý toàn bộ hệ điều hành. Trong 3 user client, có 2 user có password ít hơn 7 ký tự (4 ký tự)
4. Giả sử bạn là attacker thực hiện các hành động tấn công.

**Yêu cầu:**

Câu 1: cài đặt chương trình (1 điểm)

- Cài đặt chương trình Nmap trên máy attacker
- Cài đặt chương trình Nessus trên máy Attacker
- Cài đặt chương trình Cain&Abel
- Cài đặt ettercap

Câu 2: xác định các dịch vụ (2 điểm)

- Xác định các phiên bản hệ điều hành các máy trên mạng
- Xác định các port trên các máy
- Xác định các dịch vụ tương ứng với các port

Câu 3: sử dụng Nmap và Nessus để scan các vulnerability (2 điểm)

- Sử dụng Nmap để scan các lỗ hổng hệ điều hành
- Sử dụng Nessus để scan lỗi hệ điều hành và mạng
- Xác định các vulnerability có thể truy cập từ xa trên các máy.

Câu 4: Khai thác lỗ hổng (4 điểm)

- Sử dụng chương trình Cain&Abel or Ettercap để sniff file username và password của máy Client,
- Tiến hành crack password của các client với Cain&Abel
- Sử dụng metaploit để truy cập vào các máy với các lỗ hổng remote.

Câu 5: Hướng khắc phục (1 điểm)

- Đưa ra hướng khắc phục các lỗ hổng trên các máy.

**Lưu ý:**

- Sinh viên sử dụng tên mình đặt mật khẩu ví dụ: sinh viên A tên Mai Vân Phương Vũ → password: vumvp
- Sử dụng các hệ điều Window, backtrack, Vmware,..
- Thực hiện report từng cá nhân, không thực hiện nhóm. Chụp hình hay quay phim lại quá trình thực hiện report.
- Nghiêm cấm sao chép.