BÀI THỰC HÀNH 06

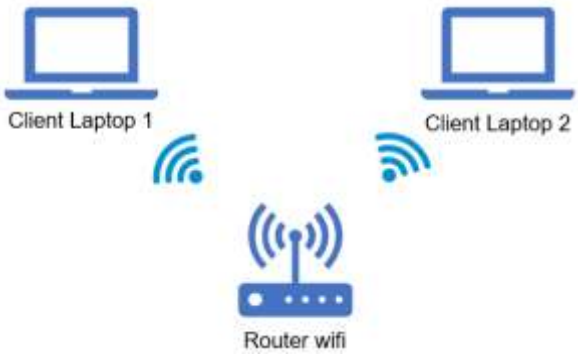
MỤC TIÊU:

Sau bài thực hành, sinh viên có khả năng thực hiện được:

- ✓ Cấu hình được chức năng dịch địa chỉ nội bộ (Inbound Address Translation - IAT)
- ✓ Hạn chế truy cập internet bằng cách sử dụng firewall
- ✓ Lọc danh sách máy trạm được truy cập mạng không dây bằng chức năng MAC Filtering
- ✓ Sử dụng được lệnh netsh advfirewall thiết lập luật trên Windows Firewall with Advanced Security
- ✓ Thiết lập được DMZ host ip address

BÀI 1 (04 ĐIỂM):

Cho sơ đồ mạng sau:



Sử dụng router wifi Linksys WRT55AG hoặc sử dụng trình giả lập của hãng tại url: https://ui.linksys.com/WRT55AG/v2/1.67

Hãy thực hiện:

- Vô hiệu hóa SSID broadcast

- Thiết lập cấu hình Inbound Address Translation để forward inbound web traffic đến một máy chủ web trong hệ thống, cấu hình theo bảng sau:

Application	Port Range	Protocol	IP Address
HTTP	80 to 80	TCP	192.168.1.10
HTTPS	443 to 443	TCP	192.168.1.10

SMTP	25 to 25	TCP	192.168.1.10

+ Chặn truy cập tới website https://www.facebook.com/

+ Chặn truy cập tới các website chứa từ khóa cụ thể trong URL hoặc tiêu đề của chúng, với từ khóa: **hack, black**

- Lọc địa chỉ MAC (MAC filtering) của 02 client, có địa chỉ MAC như sau:

+ Client1: 00-0f-66-e7-50-d1

+ Client2: 00-12-17-88-18-71

- Thiết lập DMZ host ip address tới địa chỉ 192.168.1.20

BÀI 2 (04 ĐIỂM):

Sử dụng lệnh netsh advfirewall hãy thiết lập các luật sau trên Windows Firewall with Advanced Security:

- Cấm truy cập share qua cổng TCP:445

- Cho phép ping

- Cho phép mở cổng TCP:8888

- Chặn cổng TCP:9999

- Chặn kết nối internet của phần mềm Microsoft Edge

- Chặn truy cập từ địa chỉ IP bên ngoài 89.22.34.156

- Chặn truy cập từ địa chỉ IP nội bộ

BÀI 3 (02 ĐIỂM): GIẢNG VIÊN CHO THÊM

HƯỚNG DẪN NỘP BÀI:

Sinh viên làm báo chi tiết các bước thực của bài lab và lưu lại dưới dạng file .pdf với tên file đặt theo định dạng: **lab6_MaSV.pdf**

Nộp lên hệ thống theo yêu cầu của giảng viên