**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**
**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**
**KHOA CÔNG NGHỆ THÔNG TIN**


# BÁO CÁO ĐỒ ÁN CUỐI KỲ

**Họ và tên sinh viên: Nguyễn Trí Đức**
**MSSV: 20120060**
**Môn học: An ninh máy tính**
**Năm học: 2023 – 2024**
**Lớp: 20_22**
**Giảng viên: Thầy Huỳnh Nguyên Chính**
**Thầy Nguyễn Văn Quang Huy**
**Thầy Ngô Đình Hy**

***Thành phố Hồ Chí Minh, ngày 18 tháng 1 năm 2024***

## Mục lục

# I. Báo cáo chi tiết:

## Câu 1: Thiết kế mạng cho công ty A đảm bảo tính bảo mật. *(Vẽ sơ đồ luận lý, trình bày giải pháp thiết kế)*

Công ty A gồm có trụ sở chính và 1 chi nhánh.

**Tổ chức hệ thống mạng ở trụ sở chính như sau:**

- Có Firewall (tích hợp tính năng IPS – Intrusion Prevention System: hệ thống phòng ngừa xâm nhập)
- Có WAF – Web Application Firewall để bảo vệ Web server
- Các ứng dụng nội bộ chạy trên máy chủ ứng dụng (App Server)
- Cơ sở dữ liệu đặt ở một server riêng (Database server)
- Có 5 phòng ban, mỗi phòng ban khoảng 30 người
- Có hệ thống WiFi

**Tổ chức hệ thống mạng ở chi nhánh**

- Có FW để bảo vệ hệ thống mạng LAN
- Có 2 phòng ban, mỗi phòng ban có khoảng 20 người
- Các ứng dụng truy xuất tập trung qua hệ thống của trụ sở chính.
- Có hệ thống WiFi.

Giải pháp thiết kế:

- Ứng dụng thực hiện : Cisco Packet Tracer – 8.2.1

**Các chính sách bảo mật được sử dụng cho hệ thống mạng công ty A:**

LAN security

- Port Security : cấu hình trên Switch
- DHCP Snooping: cấu hình trên Switch
- ACL:
    - Access Control List là danh sách các điều kiện điều khiển truy cập được áp đặt vào các Interface của Router/ Switch layer3 (gọi chung là Layer3 Devices) để điều khiển luồng lưu lượng đi qua nó.

- Firewall: là thiết bị được đặt để kiểm soát giữa miền có độ tin cậy cao và miền có độ tin cậy thấp (VD giữa mạng nội bộ (trusted) và mạng Internet (untrusted), hoặc thực tế hơn, Firewall sẽ được đặt giữa 3 khu vực: DMZ, Internet, Inside)
- IDS/ IPS
- Network Monitoring System

WEF: cấu hình Firewall bảo về Web Server.

Wifi security:

- Cấu hình AP giới hạn số lượng kết nối
- Cấu hình WPA2 – personal
- Cấu hình xác thực người dùng bằng Radius Server

Các giải pháp phòng chống các lỗ hổng tấn công Web như SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)

Các giải pháp bảo vệ tài khoản/ truy cập đặc quyền (Admin/Root)

**Thiết kế :**

Thiết kế cho Trụ Sở chính gồm các khu vực :

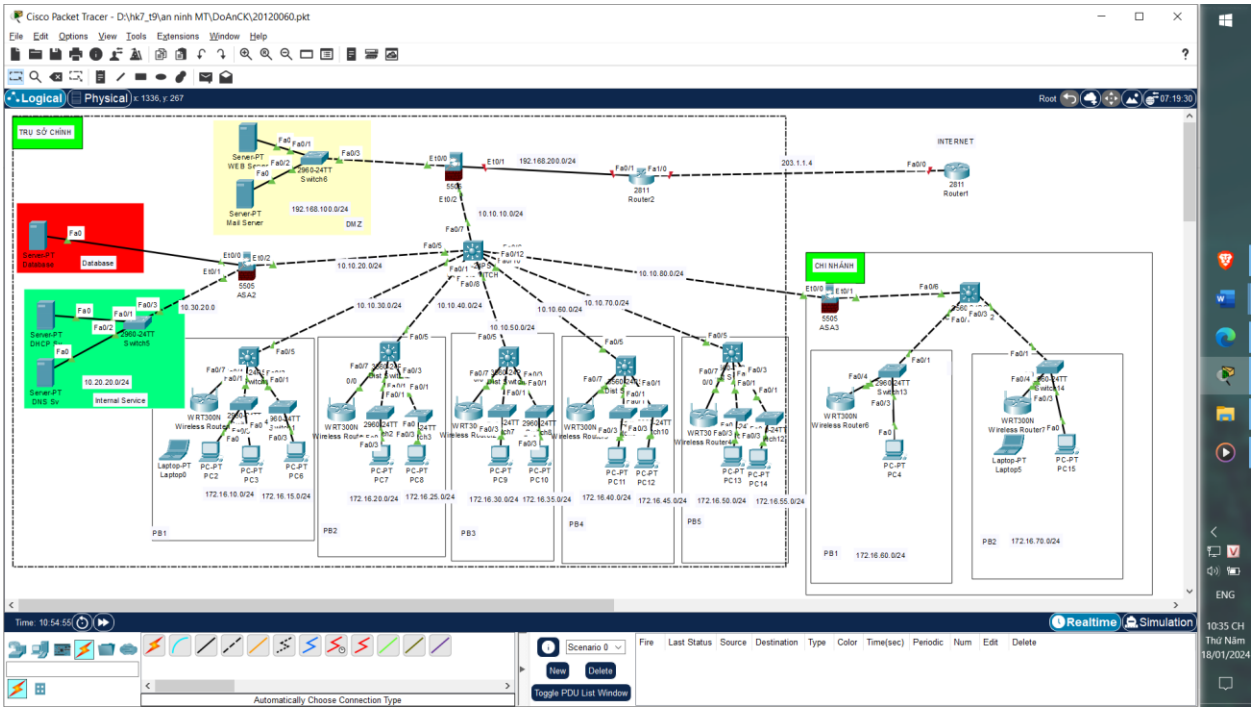
- DMZ: chứa  Web Server và Mail Server
- Database: chứa Database Server
- 2 khu vực DMZ và Database sẽ được bảo vệ bởi 1 thiết bị Firewall cài đặt riêng;
- Internal Services: chứa DHCP Server, DNS Server
- 5 phòng ban: mỗi phòng ban gồm 2 Switch kết nối với các PC, 1 Router được nối với 1 Dist Switch;

Thiết kế cho chi nhánh:

- Gồm 1 Score Switch chia ra 2 phòng ban, mỗi phòng ban gồm các user và 1 Router wifi;
- Chi nhánh sẽ được cài đặt một Firewall trung gian để kết nối đến trụ sở chính;

Chi nhánh sẽ kết nối đến một Score Switch tổng ( đặt ở trụ sở chính) , Score Switch này và khu vực DMZ sẽ phải đi qua một Firewall trước khi ra ngoài Internet,

**Mô hình luận lý:**

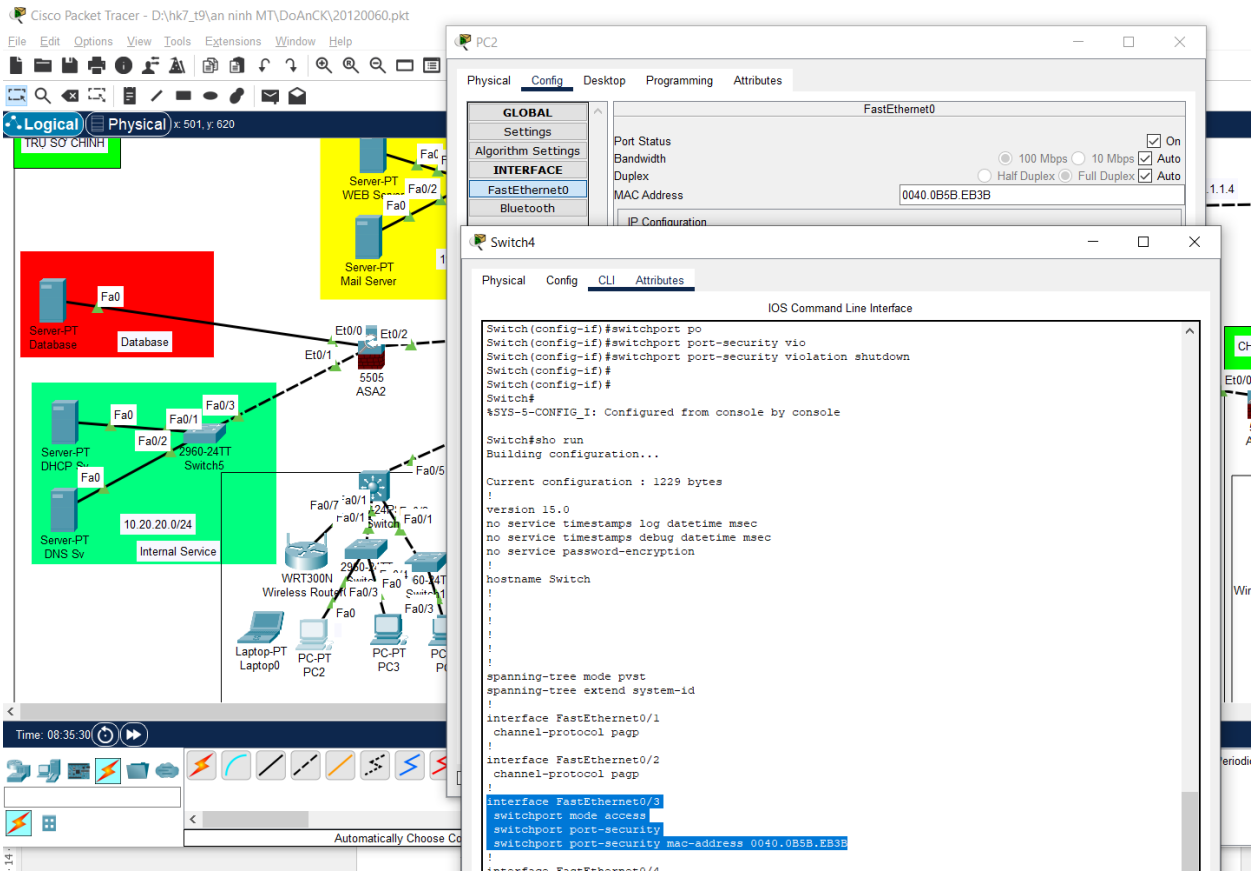



## Câu 2: Triển khai các tính năng bảo mật mạng nội bộ cho công ty A (LAN security).

***(Trình bày các kỹ thuật có thể sử dụng để an toàn trong mạng LAN, cài đặt, cấu hình)***

Triển khai Port Security – thiết bị Switch:

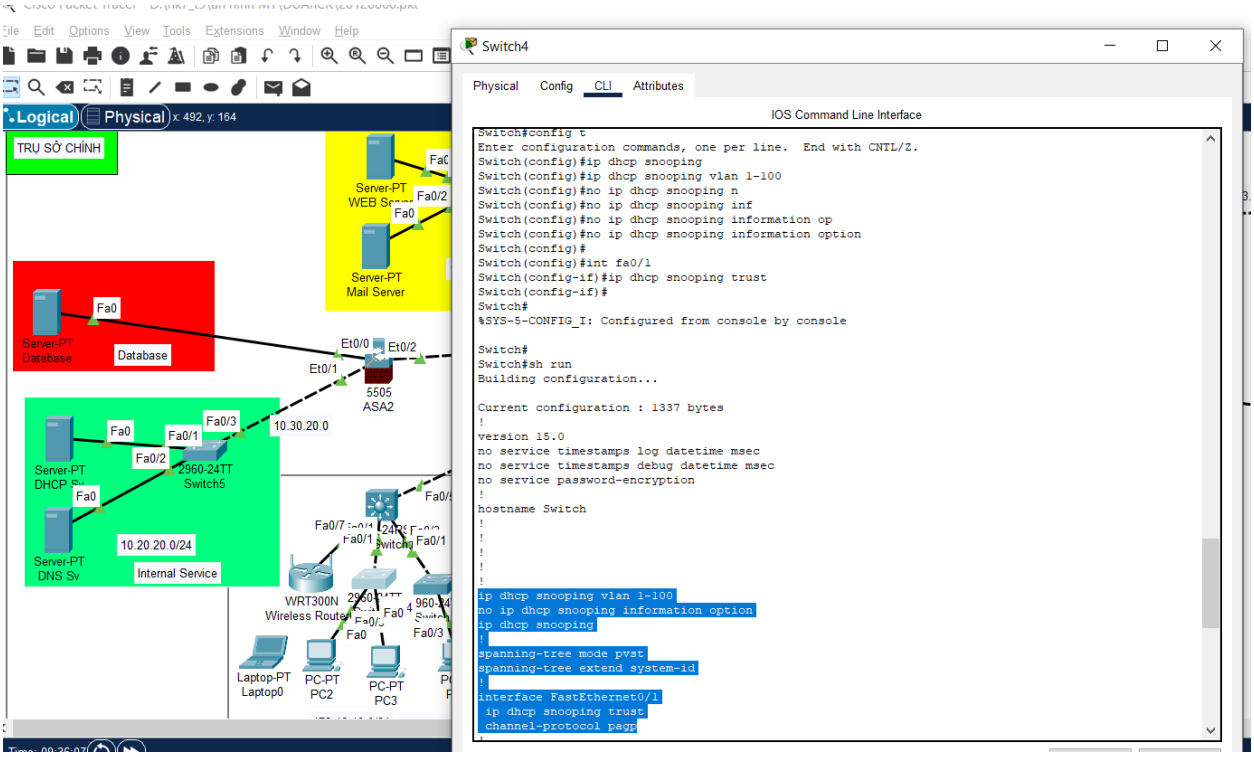
- Lấy địa chỉ MAC của PC end – user
- Vào cổng switch kết nối trực tiếp với PC đó và tiến hành cấu hình như sau:
    - SW(config)#interface (Fa0/1)
    - SW(config-if)#switchport mode access
    - SW(config-if)#switchport port-security
    - SW(config-if)#switchport port-security maximum 1
    - SW(config-if)#switchport port-security mac-address H.H.H | Sticky
    - SW(config-if)#switchport port-security violation shutdown
- Kết quả:




- Cấu hình tương tự với các cổng kết nối với các PC khác trong mạng của cả chi nhánh và trụ sở

Triển khai DHCP Snooping – thiết bị Switch:

- Cấu hình trên Switch kết nối trực tiếp với PC
- Ta tiến hành cấu hình với **cổng switch hướng về DHCP server** (khác cổng kết nối trực tiếp với PC cần DHCP Snooping) như sau:
    - SW(config)#ip dhcp snooping
    - SW(config)#ip dhcp snooping vlan 1-100
    - SW(config)#no ip dhcp snooping information option
    - SW(config)#interface (Fa0/1)
    - SW(config-if)#ip dhcp snooping trust
- Kết quả:




- Làm tương tự với các Switch kết nối trực tiếp với end-user còn lại.

Triển khai Access List Controll – triển khai trên Router

- Các bước:
    - Tạo Access List:

R(config)# access-list <#>(1-99) {permit/deny} <source> <wildcard>

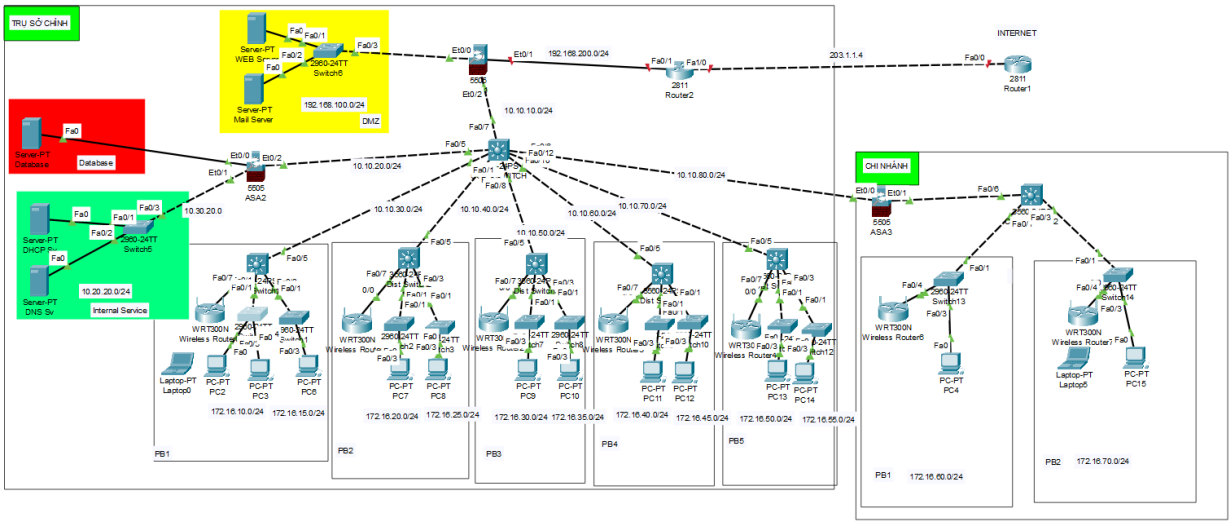
    - Áp vào Interface:

R(config)# int Fa0/0

# ip access-group 1 in/out.

Triển khai Firewall:

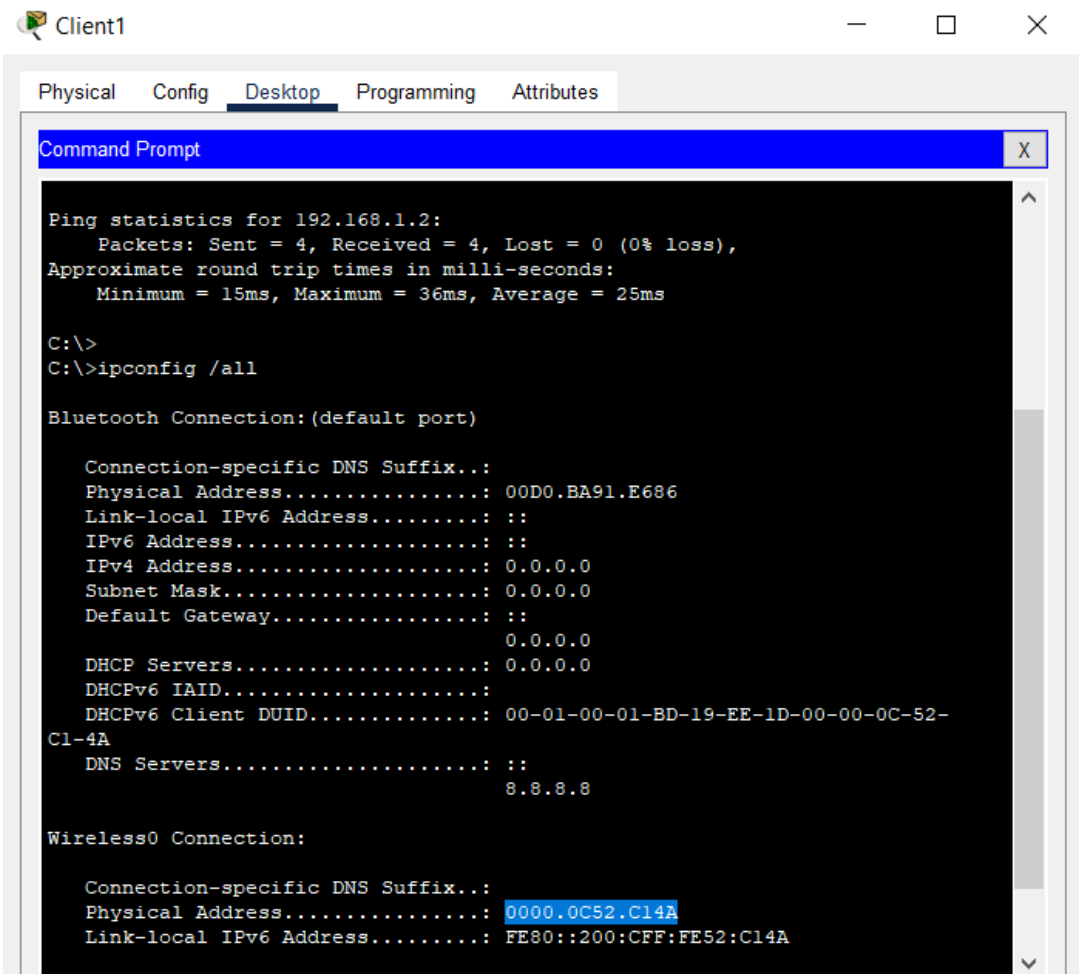
- Trong mô hình này em sẽ triển khai 3 Firewall: 1 cái để bảo vệ toàn bộ công ty, 1 cái bảo vệ Database Server và Internal Services, 1 cái để kết nối với chi nhánh, như sau:

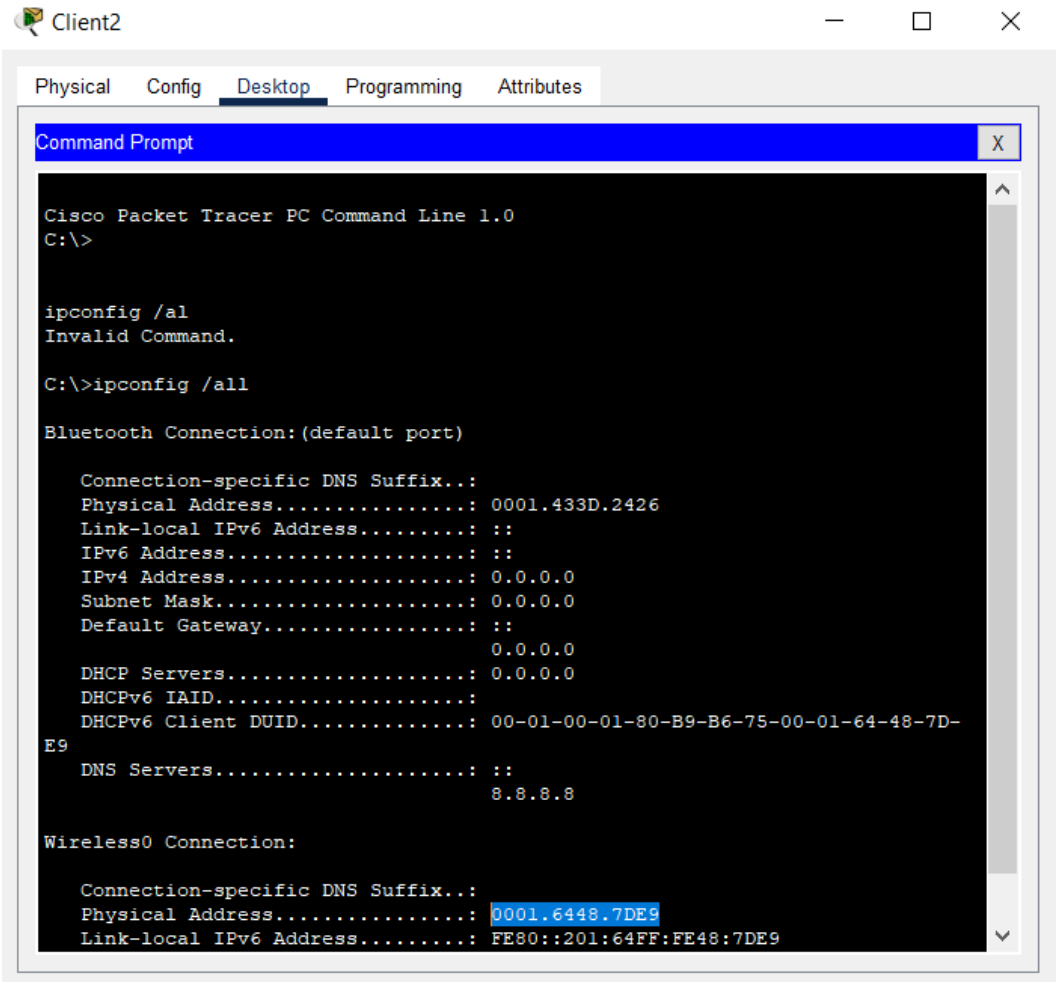


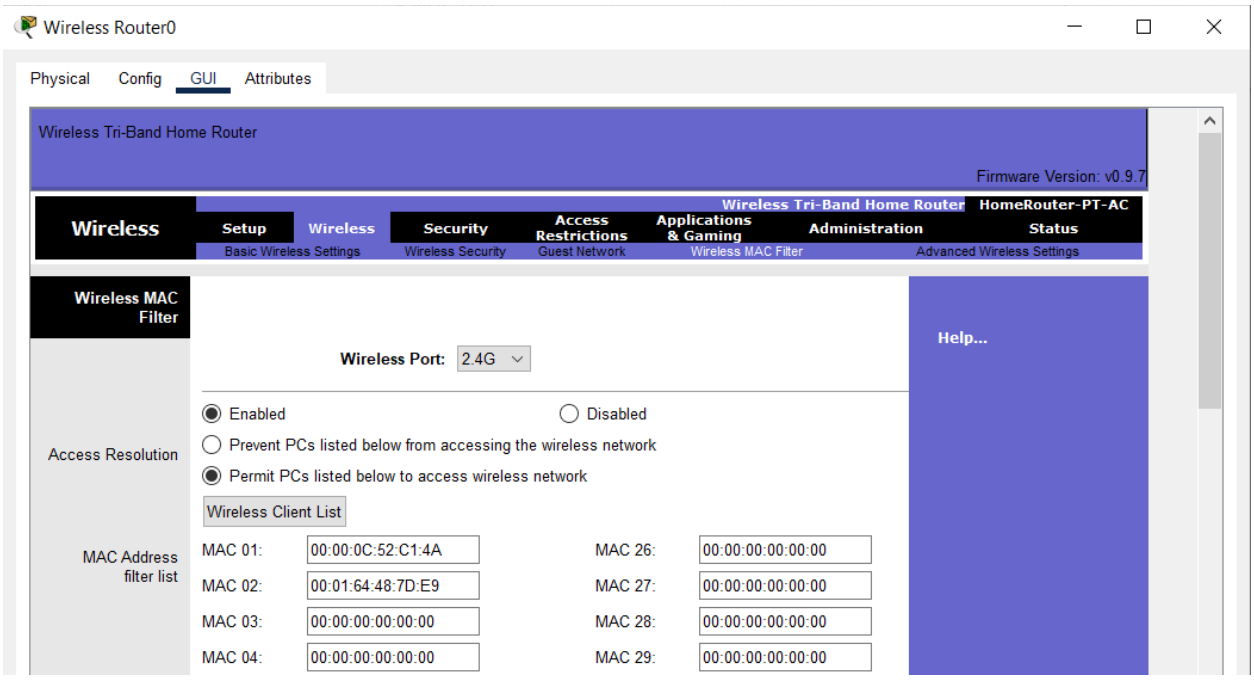

## Câu 3: Triển khai giải pháp bảo mật mạng Wifi (WiFi security). *(Trình bày các kỹ thuật có thể sử dụng để an toàn trong mạng WLAN, cài đặt, cấu hình)*

Các kỹ thuật Wifi security có thể sử dụng để an toàn cho hệ thống:

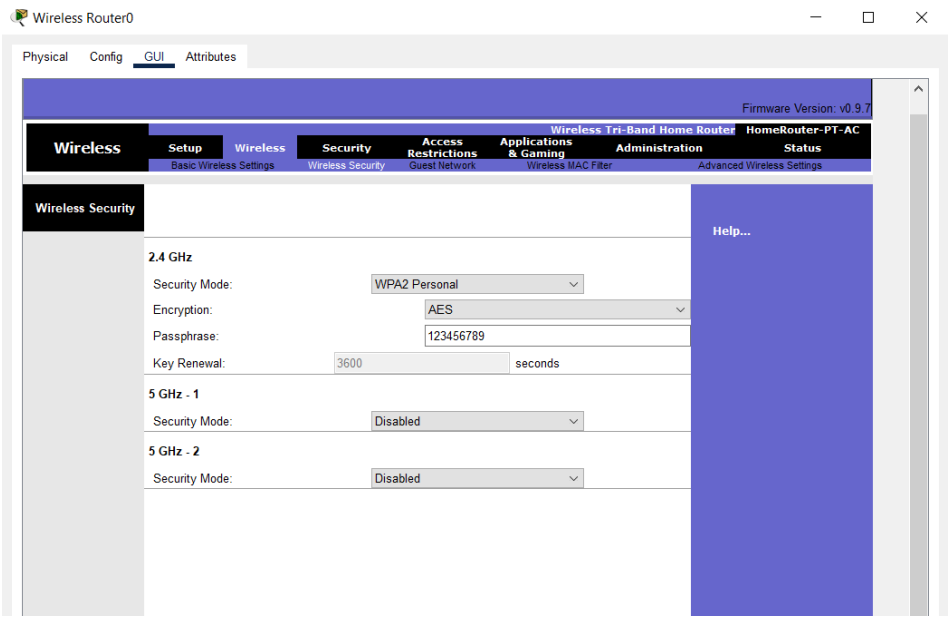
- Cấu hình Access Point giới hạn số client kết nối vào wifi ( bằng MAC filtering), các bước như sau:
    - Lấy địa chỉ MAC của những máy Client bạn muốn cho phép kết nối:
        - Destop – Command Prompt – Gõ ‘ipconfig /all’
        - Địa chỉ MAC chính là Physical Address
    - Vào Router – GUI – Wireless – Wireless MAC Filter
    - Click chọn “Permit PCs listed below to access wireless network”
    - Điền địa chỉ MAC của 2 máy cho phép kết nối – Lưu


Client1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 15ms, Maximum = 36ms, Average = 25ms
C:\>
C:\>ipconfig /all
Bluetooth Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 00D0.BA91.E686
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-BD-19-EE-1D-00-00-0C-52-
C1-4A
DNS Servers.....: ::
8.8.8.8
Wireless0 Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 0000.0C52.C14A
Link-local IPv6 Address.....: FE80::200:CFF:FE52:C14A

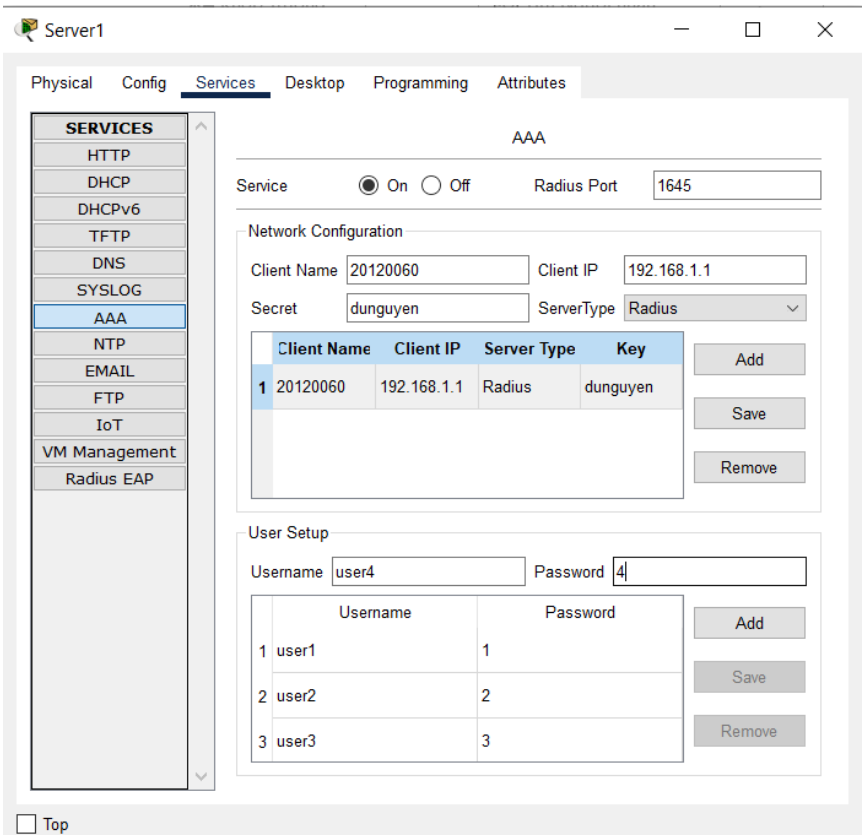

Client2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>
ipconfig /al
Invalid Command.
C:\>ipconfig /all
Bluetooth Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 0001.433D.2426
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-80-B9-B6-75-00-01-64-48-7D-E9
DNS Servers.....: ::
8.8.8.8
Wireless0 Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 0001.6448.7DE9
Link-local IPv6 Address.....: FE80::201:64FF:FE48:7DE9


Wireless Router0
Physical
Config
GUI
Attributes
Wireless Tri-Band Home Router
Firmware Version: v0.9.7
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Wireless Tri-Band Home Router
HomeRouter-PT-AC
Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Advanced Wireless Settings
Wireless MAC Filter
Help...
Wireless Port: 2.4G
Enabled
Disabled
Access Resolution
Prevent PCs listed below from accessing the wireless network
Permit PCs listed below to access wireless network
Wireless Client List
MAC Address filter list
MAC 01: 00:00:0C:52:C1:4A
MAC 02: 00:01:64:48:7D:E9
MAC 03: 00:00:00:00:00:00
MAC 04: 00:00:00:00:00:00
MAC 26: 00:00:00:00:00:00
MAC 27: 00:00:00:00:00:00
MAC 28: 00:00:00:00:00:00
MAC 29: 00:00:00:00:00:00

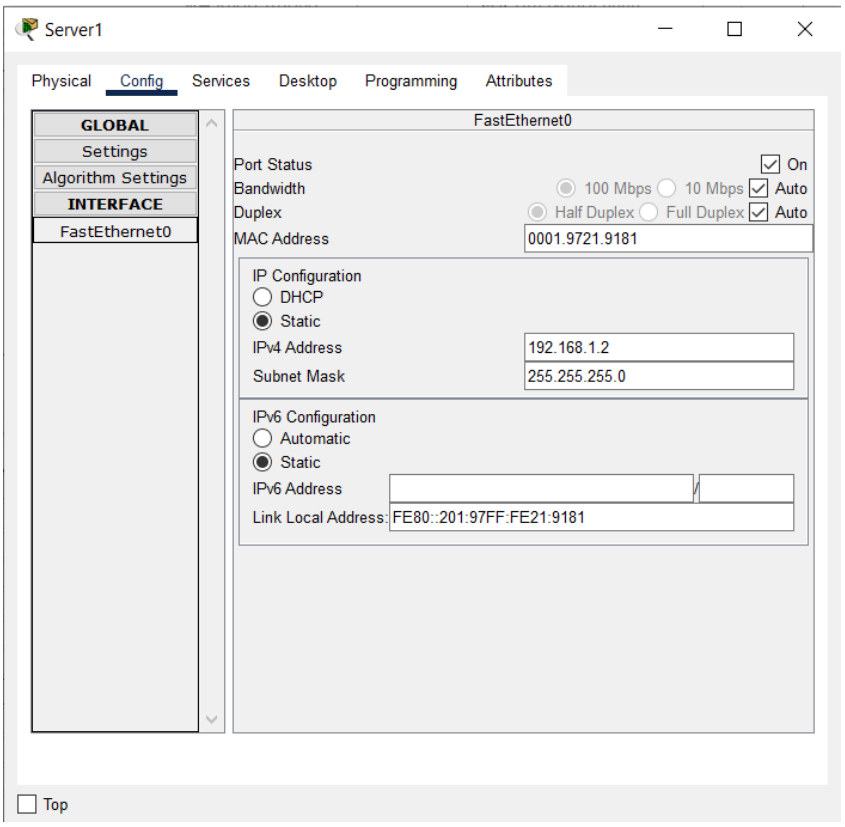
- Cấu hình WPA2 – personal (dùng password):
    - Vào Wireless – Wireless Security
    - Chọn Security Mode là WPA2 Personal
    - Đặt mật khẩu Passphrase, vd: 123456789



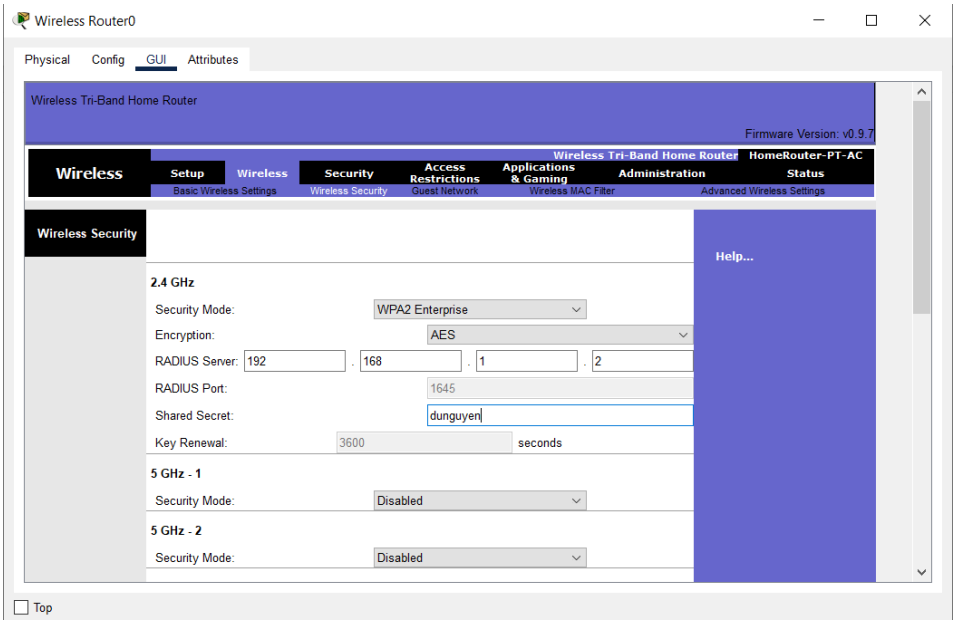

- Cấu hình chứng thực người dùng Wifi dùng Radius Server:
    - Cấu hình Authentication Server (Radius server), tạo account để chứng thực người dùng Wifi:
        - Vào End Device chọn thiết bị Server
        - Cài đặt Server:
            - Vào Services – AAA – bật Service thành “On”
            - Thiết lập thông số - Add và tạo các tài khoản cho user, ví dụ:




- Thiết lập IP Static cho Server: Config – FastEthernet0 – Chọn Static và nhập IPv4, vd: 192.168.1.2




- AP đóng vai trò là Authenticator (dùng WPA2-Enterprise)
  - Cài đặt Router:
  - Vào Wireless – Wireless Security – Chọn mod WPA2 – Enterprise
  - Thiết lập các thông số như đã cài đặt ở Server



Bên cạnh những giải pháp bảo mật trên, kẻ tấn công cũng có thể tấn công Wifi bằng các phương pháp khác, ví dụ như: Brute Force:

- Cách thức thực hiện:
    - Hacker sử dụng các công cụ tự động để thử từng mật khẩu có thể có cho mạng WiFi.
    - Tấn công có thể được thực hiện tại cổng truy cập mạng không dây hoặc từ xa.
- Mục tiêu của hacker:
    - Đoán đúng mật khẩu để có thể kết nối và xâm nhập vào mạng WiFi.
    - Tiềm ẩn rủi ro về an ninh thông tin của mạng và các thiết bị kết nối.
- Giải pháp phòng chống:
    - Sử dụng mật khẩu mạnh:
        - Khuyến khích sử dụng mật khẩu có ít nhất 12 ký tự, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt.
        - Tránh sử dụng mật khẩu dễ đoán như ngày sinh, tên hoặc các chuỗi đơn điệu.
    - Thay đổi mật khẩu định kỳ: Đặt chính sách đổi mật khẩu định kỳ, ví dụ như mỗi 3 hoặc 6 tháng một lần.
    - Sử dụng WPA3: Nếu có khả năng, chuyển từ WPA2 sang WPA3 để tận dụng những cải tiến bảo mật.
    - Giới hạn số lần đăng nhập sai:
        - Kích thích việc sử dụng cấm tạm thời sau một số lần đăng nhập sai.
        - Gửi cảnh báo hoặc thông báo cho quản trị viên khi có nhiều đăng nhập sai.
    - Tăng cường an ninh mạng WiFi:
        - Ẩn tên mạng (SSID):
            - Vô hiệu hóa hiển thị tên mạng WiFi để giảm rủi ro bị phát hiện.
            - Sử dụng MAC filtering:

- Thiết lập danh sách địa chỉ MAC được phép kết nối để ngăn chặn các thiết bị không ủy quyền.
- Cập nhật firmware và phần mềm:
- Đảm bảo rằng tất cả các thiết bị và phần mềm liên quan đều được cập nhật để khắc phục các lỗ hổng bảo mật.

- Kiểm tra log và cảnh báo:
  - Thường xuyên kiểm tra log đăng nhập để phát hiện các hoạt động đáng ngờ.
  - Cài đặt hệ thống cảnh báo để thông báo ngay lập tức khi có nhiều lần đăng nhập sai.
  - Bằng cách kết hợp những giải pháp trên, người quản trị mạng có thể tăng cường an ninh mạng WiFi và giảm rủi ro bị tấn công Brute Force

**Câu 4: Triển khai giải pháp bảo mật Web (Web security).** ***(Trình bày các kỹ thuật có thể sử dụng để an toàn cho Web, cài đặt, cấu hình)***

Những phương pháp tấn công trên Web như : SQL Injection, Cross-site Scripting Attack; Cross-site Request Forgery

SQL Injection:

- Tấn công SQL injection là một kỹ thuật tấn công mà kẻ tấn công cố gắng chèn hoặc thực hiện các câu truy vấn SQL độc hại vào các điểm nhập liệu của ứng dụng web. Nếu ứng dụng không kiểm tra và xử lý đúng cách dữ liệu nhập vào từ người dùng, người tấn công có thể thực hiện các thao tác độc hại như truy xuất, sửa đổi, hoặc xóa dữ liệu trong cơ sở dữ liệu của ứng dụng.
- Dưới đây là một số cách phổ biến để tấn công SQL injection:
  - Thực hiện tấn công thông qua biểu mẫu nhập liệu: Kẻ tấn công có thể chèn mã SQL độc hại vào các trường của biểu mẫu nhập liệu trên trang web.

- Thực hiện tấn công qua tham số URL: Khi ứng dụng sử dụng các tham số từ URL để thực hiện các câu truy vấn SQL, kẻ tấn công có thể chèn mã SQL độc hại vào các tham số đó.
- Chèn mã SQL vào cookies hoặc tiêu đề HTTP: Kẻ tấn công có thể thử chèn mã SQL độc hại vào cookies hoặc tiêu đề HTTP và xem xét xem liệu các giá trị này có được sử dụng trong câu truy vấn SQL hay không

Cross-site Scripting Attack:

- Cross-Site Scripting (XSS) là một loại tấn công mà kẻ tấn công chèn mã script độc hại vào trang web và khiến cho trình duyệt của người khác thực thi mã đó. XSS thường xuyên tận dụng các điểm đầu vào không được kiểm tra hoặc làm sạch đúng cách, chẳng hạn như các biểu mẫu nhập liệu, tham số URL, hoặc các phần nội dung của trang web.
- Một số cách thức mà kẻ tấn công thực hiện XSS:
  - Tấn công thông qua Biểu mẫu nhập liệu: Kẻ tấn công có thể chèn mã script vào các trường của biểu mẫu nhập liệu, ví dụ như ô tìm kiếm, ô đăng nhập, hay các biểu mẫu đăng ký.
  - Tấn công thông qua tham số URL: Khi ứng dụng sử dụng tham số từ URL để hiển thị dữ liệu, kẻ tấn công có thể chèn mã script vào các tham số đó, và sau đó ứng dụng hiển thị nó mà không kiểm tra.
  - Tấn công thông qua Cookies hoặc Tiêu đề HTTP: Kẻ tấn công có thể chèn mã script độc hại vào cookies hoặc tiêu đề HTTP và xem xét xem liệu giá trị này có được sử dụng trong trang web hay không.

Cross-site Request Forgery

- Cross-Site Request Forgery (CSRF) là một loại tấn công mà kẻ tấn công lừa đảo người dùng để thực hiện các hành động không mong muốn trên một trang web mà họ đã đăng nhập. Tấn công này thường xuyên nhắm vào việc sử dụng quyền đăng nhập hiện tại của người dùng để thực hiện các yêu cầu trái ngược ý muốn từ phía

họ, chẳng hạn như thay đổi thông tin tài khoản hoặc thực hiện các giao dịch tài chính.

- Một số cách thức mà kẻ tấn công có thể thực hiện CSRF:
    - Image-based CSRF (CSRF qua hình ảnh): Kẻ tấn công có thể chèn mã HTML vào trang web mà người dùng truy cập, trong đó có chứa các yêu cầu CSRF ẩn, ví dụ như sử dụng thẻ <img> với src là URL của yêu cầu CSRF.
    - Form-based CSRF: Kẻ tấn công có thể tạo các biểu mẫu ẩn hoặc ẩn điều kiện trên trang web mà người dùng truy cập, và khi người dùng thực hiện hành động như nhấn nút submit, các yêu cầu CSRF được gửi đến server mà họ đã đăng nhập.
    - Link-based CSRF: Kẻ tấn công có thể chèn liên kết chứa yêu cầu CSRF vào trang web hoặc email. Khi người dùng nhấp vào liên kết, yêu cầu CSRF sẽ được thực hiện với quyền đăng nhập của họ.

Giải pháp tăng cường Web Security:

- Xử lý code nhằm hạn chế SQL Injection:
    - Sử dụng thủ tục lưu trữ (Stored Procedures): Sử dụng thủ tục lưu trữ thay vì các câu truy vấn SQL trực tiếp. Thủ tục lưu trữ giúp ngăn chặn việc chèn mã SQL độc hại vì chúng thường không thực thi nhiều câu truy vấn.
    - Sử dụng câu lệnh tham số hóa: Sử dụng câu lệnh tham số hóa trong câu truy vấn SQL. Điều này giúp tránh được việc chèn giá trị người dùng trực tiếp vào câu truy vấn.
    - Kiểm tra và làm sạch đầu vào: Thực hiện kiểm tra và làm sạch đầu vào người dùng trước khi sử dụng nó trong câu truy vấn SQL. Sử dụng các thư viện và hàm được cung cấp bởi ngôn ngữ lập trình để ngăn chặn các kí tự đặc biệt có thể làm suy luận câu truy vấn.

    - Nguyên tắc ít quyền hạn (Principle of Least Privilege): Thiết lập quyền hạn của cơ sở dữ liệu sao cho người dùng chỉ có quyền truy cập và thực hiện những thao tác cần thiết. Không nên cấp quyền hạn lớn hơn cần thiết.
    - Sử dụng bảo vệ tầng ứng dụng (Application Firewalls): Triển khai các tường lửa ứng dụng để lọc và chặn các truy vấn SQL độc hại trước khi chúng đến được cơ sở dữ liệu.
    - Cập nhật và bảo trì hệ thống: Luôn duy trì hệ thống và cơ sở dữ liệu của bạn với các bản vá và phiên bản mới nhất để bảo vệ khỏi các lỗ hổng bảo mật đã được biết đến
- Xử lý lỗ hổng Cross-site Scripting Attack:
    - Kiểm tra và Làm sạch đầu vào: Thực hiện kiểm tra và làm sạch đầu vào người dùng trước khi sử dụng nó. Sử dụng các hàm và thư viện để loại bỏ hoặc mã hóa các kí tự đặc biệt có thể làm suy luận mã script.
    - Mã hóa đầu ra: Mã hóa đầu ra trước khi hiển thị nó trên trang web. Điều này giúp tránh được việc thực thi mã script chèn vào dữ liệu người dùng.
    - Sử dụng Content Security Policy (CSP): Thiết lập CSP để xác định từ đâu các nguồn tài nguyên được tải. CSP giúp ngăn chặn việc chèn mã script bằng cách chỉ chấp nhận các nguồn đáng tin cậy.
    - HTTPOnly và Secure cho Cookies: Đặt cờ HttpOnly và Secure cho cookie. Cờ HttpOnly ngăn chặn mã JavaScript truy cập cookie, trong khi Secure chỉ cho phép truyền cookie qua kết nối an toàn (HTTPS).
    - Kiểm tra Bảo mật Trình duyệt: Sử dụng các công cụ kiểm tra bảo mật trình duyệt để phát hiện và giải quyết lỗ hổng XSS.
    - Bảo trì và Cập nhật Hệ thống: Luôn duy trì và cập nhật hệ thống với các bản vá và phiên bản mới nhất để đối phó với các lỗ hổng bảo mật đã biết đến
- Xử lý lỗ hổng Cross-Site Request Forgery

- Sử dụng CSRF Tokens: Tạo và sử dụng CSRF tokens trong mỗi yêu cầu, được tích hợp vào biểu mẫu hoặc gửi kèm với mỗi yêu cầu. Token này phải được kiểm tra để đảm bảo rằng yêu cầu được gửi là hợp lệ.
- Kiểm tra SameSite Cookies Attribute: Sử dụng thuộc tính SameSite cho cookies để giảm rủi ro của CSRF. Đặt giá trị SameSite thành "Strict" hoặc "Lax" sẽ giảm khả năng một trang web khác có thể sử dụng cookie của người dùng trong trường hợp CSRF.
- Kiểm tra Origin Headers: Sử dụng HTTP headers như Origin hoặc Referer để kiểm tra xem yêu cầu có đến từ một nguồn tin cậy hay không. Tuy nhiên, lưu ý rằng các giá trị này có thể bị giả mạo.
- Xác thực và Ủy quyền: Yêu cầu xác thực và ủy quyền chặt chẽ để đảm bảo rằng người dùng chỉ có thể thực hiện các hành động mà họ được phép.
- Tắt JavaScript trong Email: Một số email clients tự động thực thi JavaScript trong email. Tắt JavaScript trong email có thể giảm rủi ro của tấn công CSRF dựa trên email.
- Thời gian sống ngắn cho Session: Đặt thời gian sống ngắn cho session để giảm thời gian hiệu lực của cookie đăng nhập, từ đó giảm khả năng thực hiện CSRF.
- Sử dụng Content Security Policy (CSP): Thiết lập CSP để giới hạn việc tải các nguồn tài nguyên và giảm khả năng thực hiện các hành động không mong muốn từ các nguồn không an toàn

Ngoài các các trên, chúng ta cũng có thể thực hiệ n tích hợp “Mod security” cho Web Application Server để chống lại các cuộc tấn công, thông qua link tham khảo sau: https://viblo.asia/p/tich-hop-mod-security-cho-web-application-server-de-chong-lai-sql-injection-va-tan-cong-xss-bJzKmx6X59N

## Câu 5: Giải pháp bảo vệ tài khoản/truy cập đặc quyền (Administrator/root) cho hệ thống trên

Bảo vệ tài khoản với đặc quyền quản trị (Administrator/root) là một phần quan trọng của chiến lược bảo mật cho hệ thống mạng của một công ty. Dưới đây là một số giải pháp để đảm bảo an toàn cho tài khoản và truy cập có đặc quyền cao như Administrator hoặc root:

- Sử dụng tài khoản quản trị riêng biệt: Sử dụng tài khoản riêng biệt cho mục đích quản trị, không sử dụng tài khoản thông thường cho các công việc quản lý hệ thống
- Mật khẩu mạnh mẽ:
    - Đặt mật khẩu mạnh và độ dài cao cho tài khoản quản trị.
    - Thực hiện chính sách đổi mật khẩu định kỳ và không sử dụng mật khẩu dễ đoán
- Chính sách khóa tài khoản
    - Thiết lập chính sách khóa tài khoản sau một số lần nhập sai mật khẩu.
    - Thông báo cho người quản trị khi có các sự cố đăng nhập không hợp lệ
- Chứng thực 2 yếu tố (2FA) hoặc đa yếu tố (MFA):
    - Kích hoạt chứng thực hai yếu tố để cung cấp lớp bảo mật bổ sung.
    - Sử dụng mã xác minh, thiết bị thông minh hoặc ứng dụng xác thực
- Giới hạn quyền truy cập:
    - Chỉ cấp đặc quyền cần thiết cho nhiệm vụ cụ thể, tránh cung cấp quyền truy cập không cần thiết.
    - Theo dõi và đánh giá định kỳ quyền truy cập được cấp phép
- Theo dõi và ghi nhật ký ( Logging):
    - Bật chế độ ghi nhật ký để theo dõi hoạt động của tài khoản quản trị.
    - Theo dõi sự kiện đăng nhập, đăng xuất và các thay đổi đặc quyền.
- Tự động hóa và quản lý quy trình (IAM):

    - Sử dụng hệ thống IAM để quản lý và tự động hóa quy trình cấp quyền và thu hồi quyền.
    - Tự động hóa việc quản lý chu kỳ cuộc sống tài khoản
- Kiểm tra bảo mật tương thích ( Security Compliance Checks):
    - Thực hiện kiểm tra bảo mật định kỳ để đảm bảo rằng tất cả các tài khoản quản trị tuân thủ chính sách bảo mật.
    - Sử dụng công cụ quét và kiểm tra để xác minh sự tuân thủ
- Hạn chế truy cập từ xa:
    - Nếu có thể, hạn chế truy cập từ xa vào tài khoản quản trị.
    - Sử dụng VPN hoặc các giải pháp an toàn để bảo vệ truy cập từ xa
- Cập nhật và bảo dưỡng hệ thống:
    - Luôn duy trì hệ thống và phần mềm lên phiên bản mới nhất để bảo vệ khỏi các lỗ hổng bảo mật đã biết.

## II. Link video thuyết trình:

https://drive.google.com/drive/folders/1EK4PgHJcdbwWZ7JdvkyS81qALwFBkaOF?usp=drive_link

## III. Tham khảo:


- Tài liệu tham khảo môn học
- https://www.youtube.com/watch?v=berWcgiJ_p4
- https://www.youtube.com/watch?v=ukxSsqH7T0I
- https://www.youtube.com/watch?v=tS6QOxIUb6k
- https://www.youtube.com/watch?v=wh3DDFLRNqo
- https://viblo.asia/p/tich-hop-mod-security-cho-web-application-server-de-chong-lai-sql-injection-va-tan-cong-xss-bJzKmx6X59N
- https://www.youtube.com/watch?v=tS6QOxIUb6k
- ChatGPT