TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN – ĐHQG_HCM
KHOA CÔNG NGHỆ THÔNG TIN

An ninh máy tính

Đồ án cuối kỳ

Giảng viên: **Huỳnh Nguyên Chính**
Nguyễn Văn Quang Huy
Ngô Đình Hy

MSSV	**Họ và tên**
20120083	Nguyễn Trọng Hiếu

Mục đích

Kịch bản

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

- Có Firewall (tích hợp tính năng IPS)
- Có WAF 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

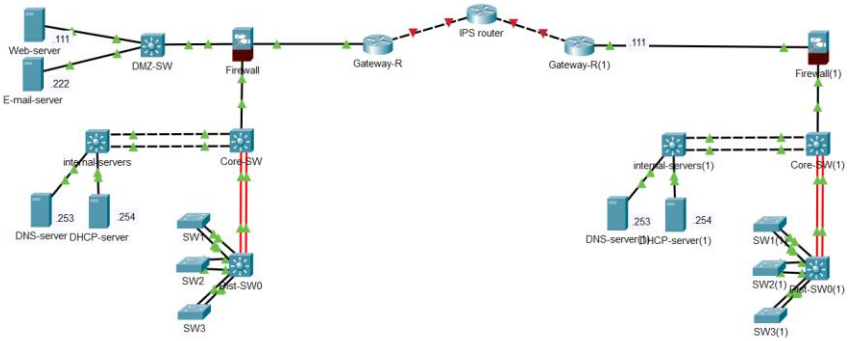
Tổ chức hệ thống mạng ở chi nhánh

- 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

Thiết kế hệ thống

1. Hệ thống mạng cho công ty A

Sơ đồ luận lý - Cisco packet tracer



Hình 1: Mô hình chung cho 2 trụ sở

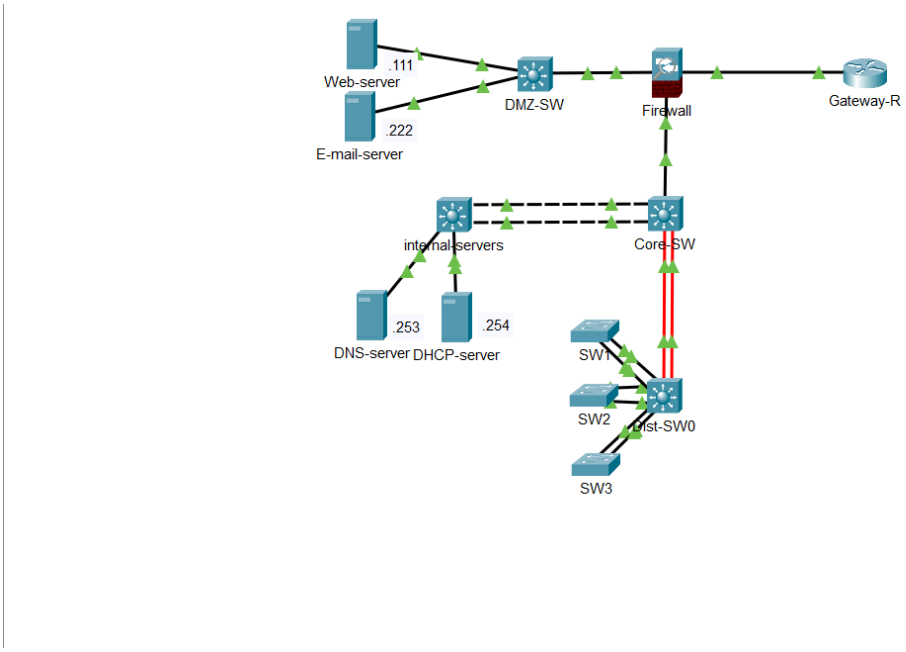
Trình bày pháp thiết kế:

1. Trụ sở chính

- Phụ thuộc vào kinh tế, và định hướng mở rộng cho hệ thống của công ty mà có các thiết kế mang tính dài/ngắn hạn tương ứng.
- Yêu cầu phần cứng và các lưu ý
    - Router: chọn router có băng thông phù hợp với nhu cầu sử dụng mạng của công ty.
    - Firewall: Đảm bảo các vùng DMZ, in/out-side được cập nhật các access-list phù hợp với mục đích nội bộ của công ty.
    - Server: Có thể thiết lập các dịch vụ (server-logic) chạy trên cùng một server-physical tại các port khác nhau.
    - Switch: số lượng switch phụ thuộc vào số lượng cổng trên một switch. Nếu có mong muốn tối ưu hóa về mặt tài nguyên thì có thể tiến hành chia VLAN cho witch để có thể tận dụng số cổng dư (3 switch cho 2 phòng ban).
    - Acesspoint – WLAN: phụ thuộc và hạ tầng của công ty mà có thể tiến hành đặt các AP tới các địa điểm quan trong (dựa trên mật độ người dùng và tần suất dùng). Cố gắng hạn chế số lượng host truy cập trên 1 AP < 40 hosts.
- Tính đồng bộ của hệ thống

- Do thiết lập trên chi nhánh yêu cầu truy suất tập trung thông qua trụ sở chính nên cần có các thiết lập cơ chế đồng bộ dự liệu một cách hợp lý khi xuất hiện thêm nhiều chi nhánh.

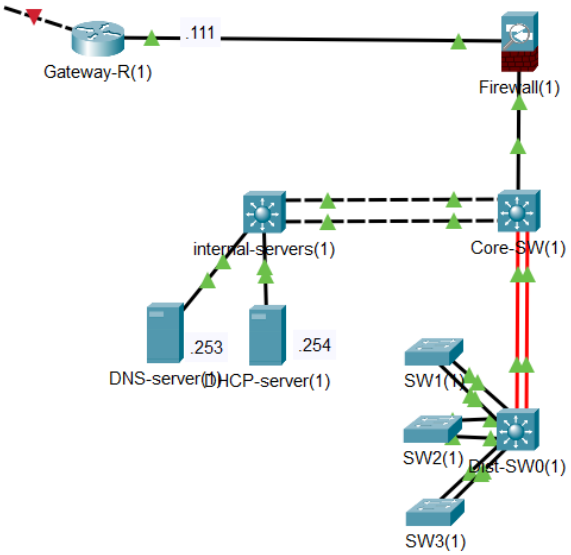
- Hệ thống giám sát quản lý
  - Phụ thuộc vào chính sách của của công ty trên phương diện quyền truy cập dữ liệu cho từng phòng ban, chi nhánh/trụ sở chính.
  - Phân vùng hệ thống giám sát cho LAN
  - Phân vùng, quyền truy cập cho từng phòng ban nhằm đảm bảo truy cập hợp lý (không vượt quyền truy cập).
- Cài đặt/Cấu hình: Tham khảo lab1



Hình 2: Kiến trúc cơ bản bên trọng trụ sở chính

2. Chi nhánh

- Yêu cầu về phần cứng:
  - Router: chọn router có băng thông phù hợp với nhu cầu sử dụng mạng của công ty.
  - Switch: số lượng switch phụ thuộc vào số lượng cổng trên một switch. Nếu có mong muốn tối ưu hóa về mặt tài nguyên thì có thể tiến hành chia VLAN cho witch để có thể tận dụng số cổng dư (3 switch cho 2 phòng ban).
  - Server: Có thể thiết lập các dịch vụ (server-logic) chạy trên cùng một server-physical tại các port khác nhau.
  - Acesspoint – WLAN: phụ thuộc và hạ tầng của công ty mà có thể tiến hành đặt các AP tới các địa điểm quan trong (dựa trên mật độ người dùng và tần suất dùng). Cố gắng hạn chế số lượng host truy cập trên 1 AP < 40 hosts.
- Cài đặt/Cấu hình: Tham khảo lab1



Hình 3: Kiến trúc cơ bản của chi nhánh công ty

2. Giải pháp bảo mật nội bộ (LAN) cho công ty A

3. Giải pháp bảo mật mạng Wifi

Đặt ra các vấn đề làm mất an toàn wifi

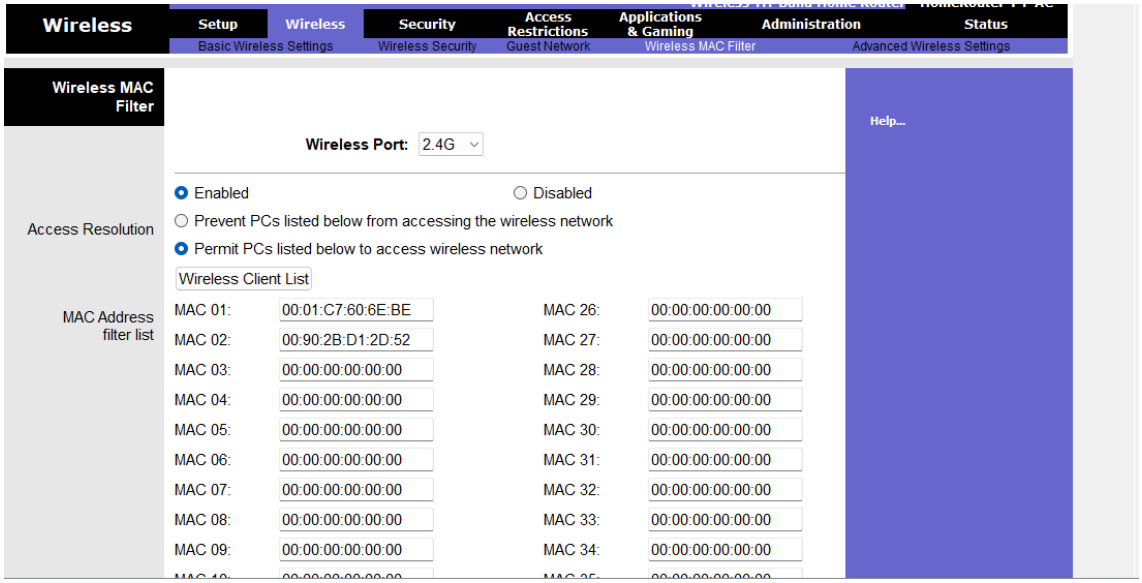
1. Lộ mật khẩu
2. Giao thức mã hóa kém
3. Tính năng có sẵn trên wifi có thể bị khai thác (WPS – Wifi Protected Setup)
4. Nhiễu do số lượng thiết bị kết nối lớn

Trình bày các kỹ thuật sử dụng

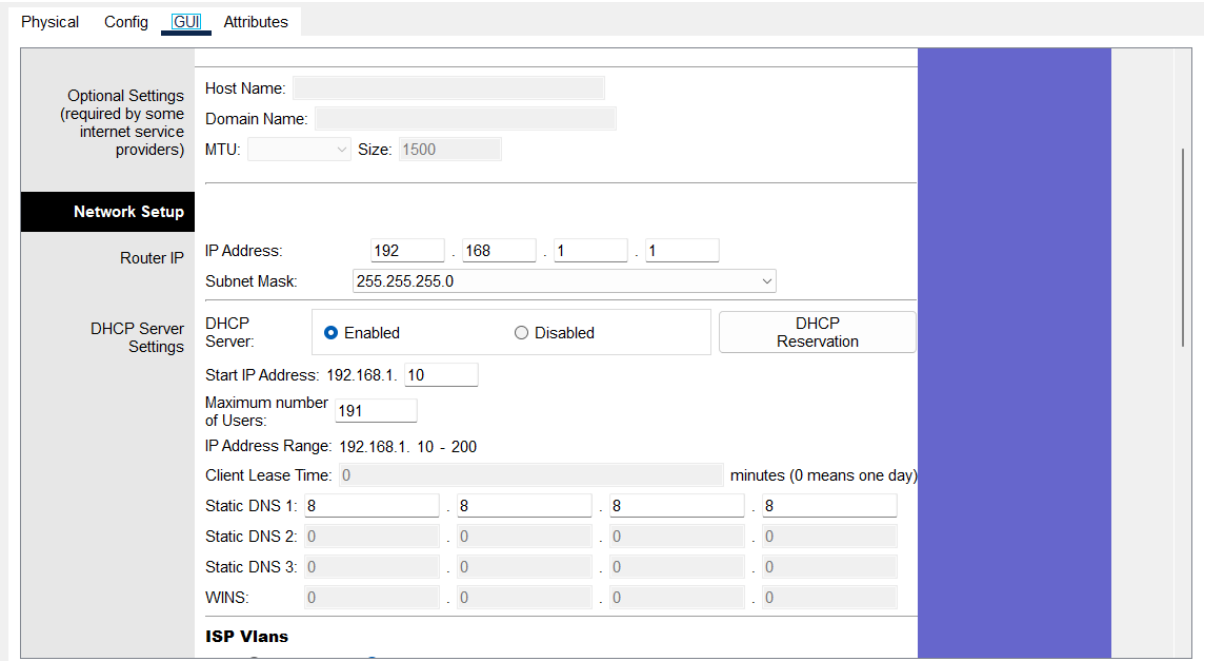
1. ***Sử dụng mật khẩu mạnh***. Mật khẩu được đánh giá an toàn khi đảm bảo các yếu tố sau đây (link):
    a. Ít nhất 12 ký tự nhưng 14 hoặc nhiều hơn là tốt hơn.
    b. Kết hợp chữ in hoa, chữ thường, số và ký tự đặc biệt.
    c. Không phải là một từ có thể được tìm thấy trong từ điển hoặc tên của một người, nhân vật, sản phẩm, hoặc tổ chức.
    d. Phải khác biệt đáng kể so với mật khẩu trước đó của bạn.
    e. Dễ nhớ đối với bạn nhưng khó đoán đối với người khác. Cân nhắc sử dụng một cụm từ dễ nhớ như "6MonkeysRLooking^".
2. ***Sử dụng mức độ mã hóa cao nhất có thể, như WPA2/3***, để bảo vệ truyền dữ liệu không dây khỏi bị đánh cắp.
3. ***Thiết lập giới hạn số lượng thiết bị có thể kết nối*** đồng thời để ngăn chặn tấn công từ quá nhiều kết nối đồng thời. It hơn 40 host trên 1 access point.
4. ***Kích hoạt tính năng tường lửa trên wireless-router*** để kiểm soát và giám sát lưu lượng mạng.

Cài đặt/Cấu hình

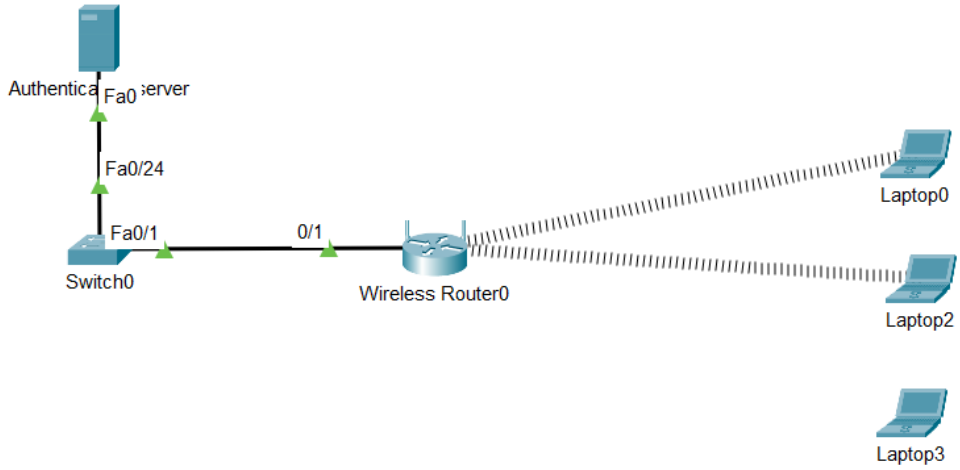
Cài đặt trên Cisco packet traver, Cấu hình theo hướng dẫn của lab Wifi security.



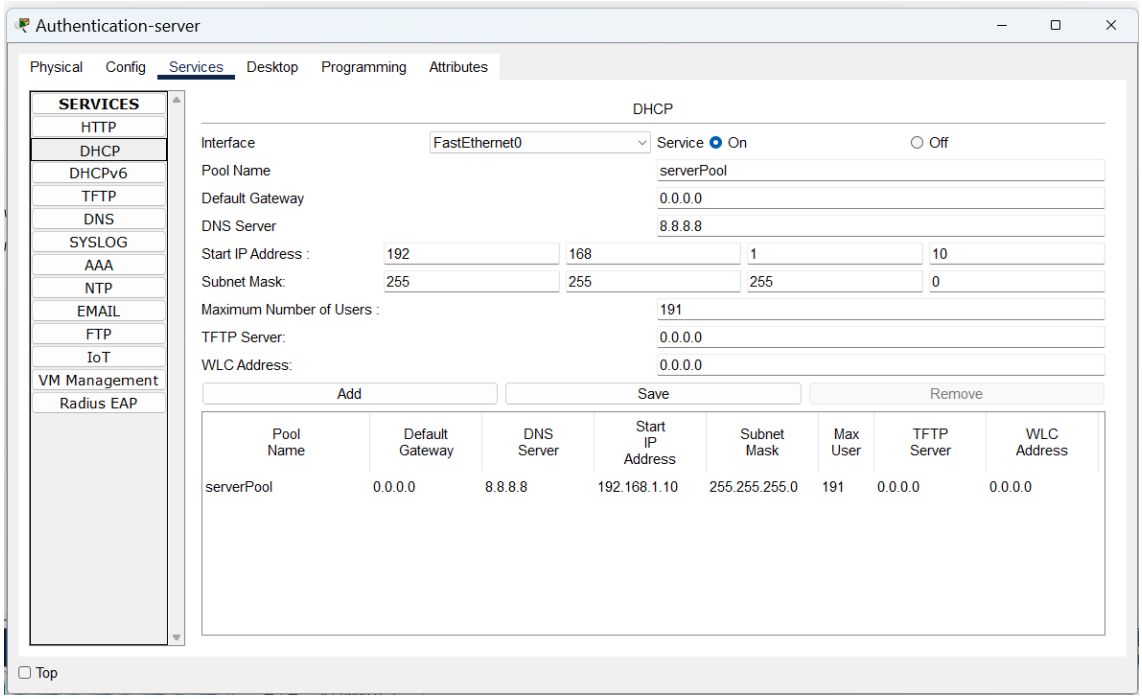
Hình 4: Cấu hình MAC filtering



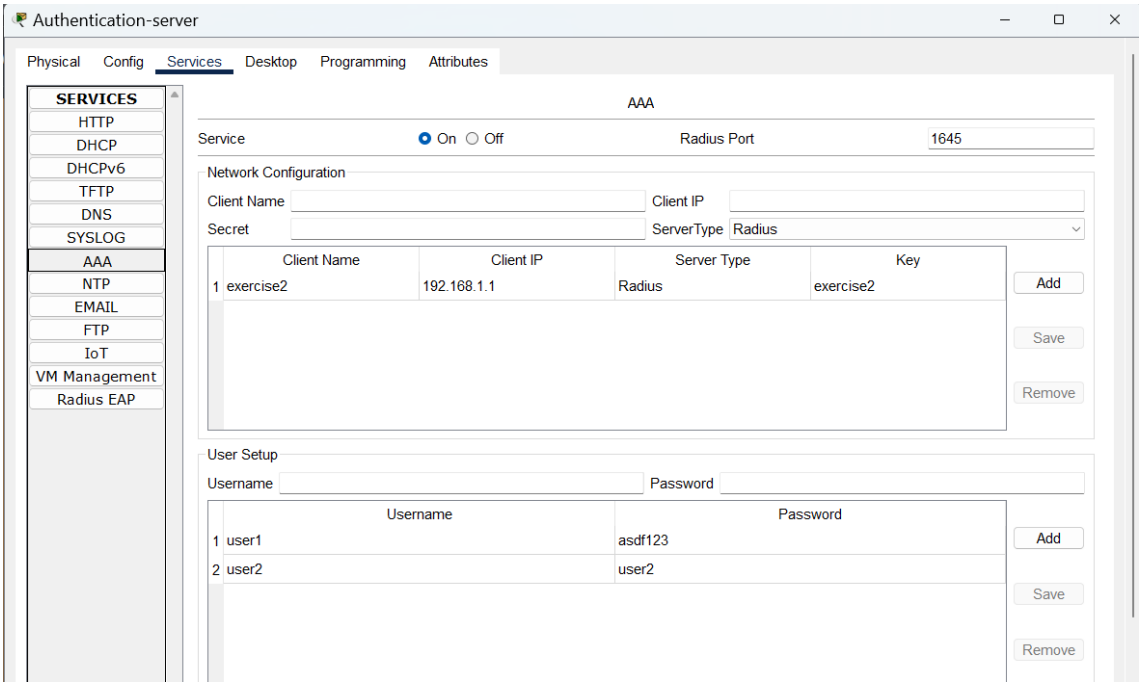
Hình 5: Thông tin địa chỉ IP



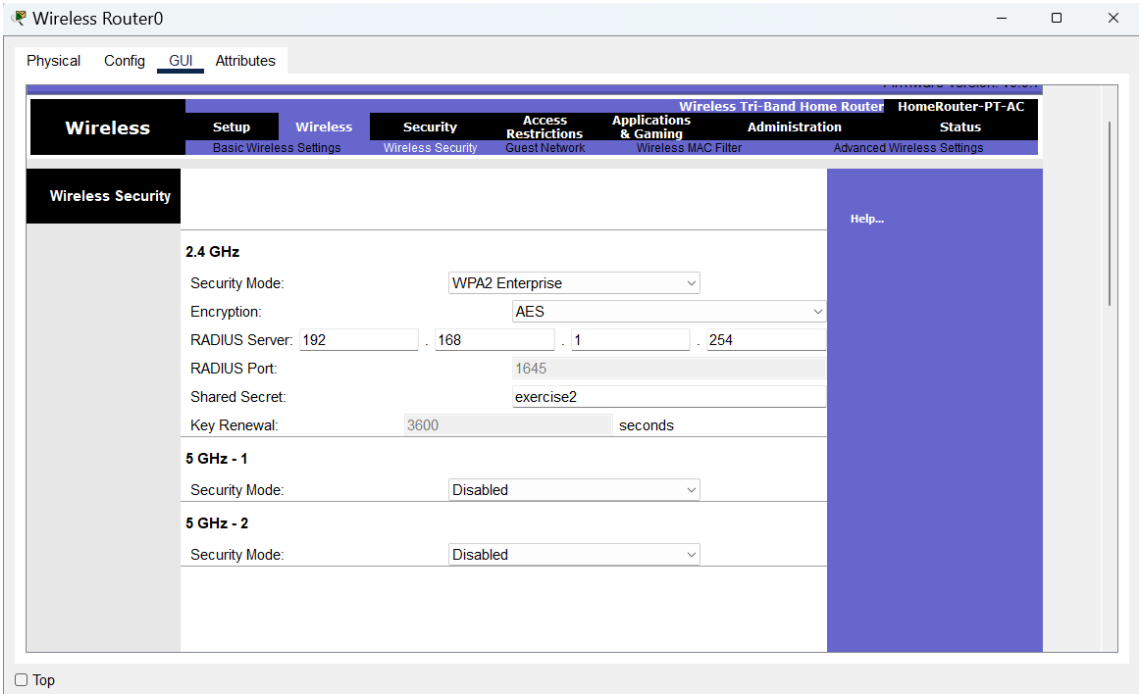
Hình 6: Mô hình Authentication server



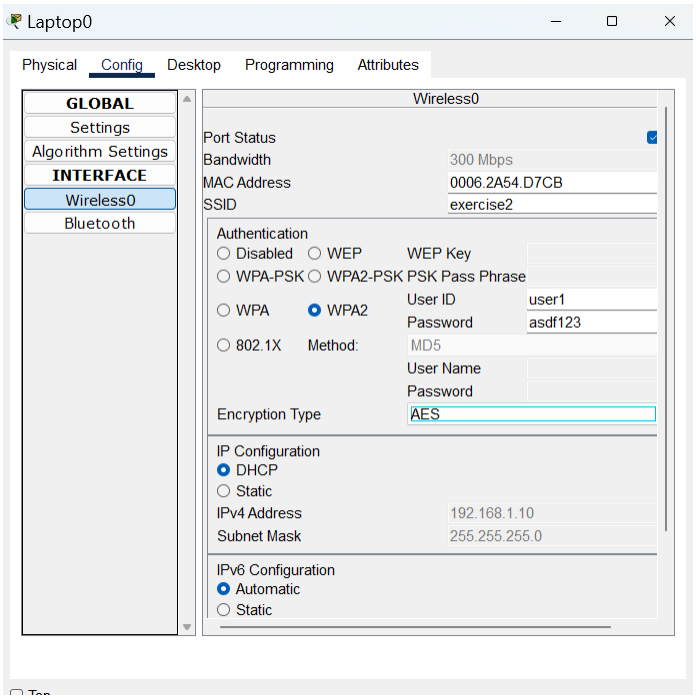
Hình 7: Cấu hình đồng thời dịch vụ DHCP trên server



Hình 8: Cấu hình Radius server trên Authentication-server



Hình 9: Thêm ip của radius-server trên Wireless router gui



Hình 10: Cấu hình wireless trên laptop để bắt được wifi

4. Giải pháp bảo mật web

Đặt ra các vấn đề làm mất an toàn web

Dựa trên OWASP top 10:

1. ***Broken Access Control***: bao gồm các lỗ hổng liên quan
    a. ***Unauthorized Data Access***: Người dùng có thể có khả năng truy cập dữ liệu nhạy cảm mà họ không được phép xem.
    b. ***Unauthorized Functionality Access***: Người dùng có thể có khả năng thực hiện các chức năng hay hành động mà họ không được phép thực hiện, chẳng hạn như xóa dữ liệu, thay đổi cài đặt hay thực hiện các thao tác quản trị.
    c. ***Elevation of Privilege***: Khi một người dùng có thể nâng cao đặc quyền của mình lên mức cao hơn so với mức đặc quyền được gán ban đầu.
2. ***Cryptographic Failures***: Là rủi ro về lỗi mật mã và dữ liệu nhạy cảm, các lỗi liên quan đến mật mã.
3. ***Injection***: Bao gồm các lỗ hổng liên quan
    a. ***SQL Injection (SQLi)***: Thông thường xảy ra trong các ứng dụng sử dụng cơ sở dữ liệu SQL. Khi người tấn công chèn các đoạn mã SQL độc hại vào các truy vấn SQL, họ có thể thực hiện các thao tác không hợp lệ trên cơ sở dữ liệu.
    b. ***Cross-site Scripting (XSS)***: Khi người tấn công chèn mã JavaScript độc hại vào các trang web hoặc ứng dụng web, thường thông qua các điểm đầu vào như biểu mẫu hoặc các tham số URL. Điều này có thể dẫn đến việc thực hiện các hành động độc hại trên trang web cho người dùng khác.
    c. ***Command Injection***: Thường xảy ra trong các hệ thống sử dụng các hàm gọi hệ thống từ dữ liệu người dùng, như khi chạy các lệnh từ dữ liệu nhập từ người dùng vào hệ thống.
    d. ***LDAP Injection***: Liên quan đến các tấn công vào hệ thống sử dụng dịch vụ Lightweight Directory Access Protocol (LDAP) để quản lý thông tin định danh của người dùng và tài nguyên trong một mạng.
4. ***Insecure Design***: tập trung vào rủi ro liên quan đến thiết kế kém chất lượng.

5. ***Security Misconfiguration***: rủi ro bảo mật trong đó cấu hình hệ thống, ứng dụng hoặc các thành phần khác của môi trường không được thiết lập chặt chẽ và an toàn. Rủi ro này thường xảy ra khi các cài đặt mặc định hoặc không an toàn được giữ lại, và thông tin quan trọng như mật khẩu, quyền truy cập, hoặc tài nguyên hệ thống có thể bị lộ ra ngoài.
6. ***Vulnerable and Outdated Components***: vấn đề khó kiểm thử và đánh giá rủi ro.
7. ***Identification and Authentication Failures***: các lỗi liên quan đến xác định người dùng
8. ***Software and Data Integrity Failures***: tập trung vào giả định không kiểm tra tính toàn vẹn của phần mềm và dữ liệu quan trọng.
9. ***Security Logging and Monitoring Failures***: là một rủi ro bảo mật liên quan đến việc không đạt được hoặc thất bại trong việc ghi log và giám sát (monitoring) các sự kiện an ninh quan trọng trong hệ thống. Quá trình này là quan trọng để phát hiện và đối phó với các hành động độc hại, tấn công, hay những tình huống không mong muốn.
10. ***Server-Side Request Forgery***: là một loại tấn công bảo mật trong đó kẻ tấn công có khả năng gửi các yêu cầu từ máy chủ (server) tới các địa chỉ mạng hay máy chủ khác, thường là qua các giao thức như HTTP hoặc DNS. Tấn công SSRF thường xảy ra khi ứng dụng web không kiểm soát được các đầu vào từ người dùng và cho phép chúng nhập các URL hoặc địa chỉ IP để thực hiện các yêu cầu từ phía máy chủ.

Trình bày các kỹ thuật sử dụng

- Sử dụng OWASP Modsecurity Core Rule Set.
- Public rules: core-rule-set
- Tiến hành cài đặt web-server apache2 trên linux có tích hợp WAF ModSecurity

Cài đặt/Cấu hình

Thực hiện trên virtualbox – kali_os, với web server apache2, tiến hành cài đặt theo hướng dẫn: link

5. Giải pháp bảo vệ tài khoản/truy cập quyền (Administrator/root)

1. ***Sử dụng mật khẩu mạnh***. Mật khẩu được đánh giá an toàn khi đảm bảo các yếu tố sau đây (link):
   a. Ít nhất 12 ký tự nhưng 14 hoặc nhiều hơn là tốt hơn.
   b. Kết hợp chữ in hoa, chữ thường, số và ký tự đặc biệt.
   c. Không phải là một từ có thể được tìm thấy trong từ điển hoặc tên của một người, nhân vật, sản phẩm, hoặc tổ chức.
   d. Phải khác biệt đáng kể so với mật khẩu trước đó của bạn.
   e. Dễ nhớ đối với bạn nhưng khó đoán đối với người khác. Cân nhắc sử dụng một cụm từ dễ nhớ như "6MonkeysRLooking^".
2. ***Xác thực Hai Yếu Tố (2FA), xác thực Đa Yếu Tố (MFA) hoặc cơ chế SSO***: Kích hoạt xác thực hai yếu tố để bổ sung lớp bảo vệ bằng cách yêu cầu một phương tiện xác thực bổ sung như mã OTP hoặc thiết bị xác minh. Sử dụng các biện pháp sinh trắc học, …
3. ***Giới hạn quyền truy cập một cách hợp lý:*** Tránh cấp toàn quyền cho một tài khoản admin, phòng trường hợp gặp phải việc leo thang đặc quyền (privilege escalation).
4. ***Kiểm tra và ghi Log***: Bật và kiểm tra các log hệ thống để theo dõi hoạt động của tài khoản quản trị, cảnh báo và phản ứng nhanh chóng đối với các hoạt động đáng ngờ.
5. ***Kiểm Soát Đầu Ra***: Kiểm tra và kiểm soát dữ liệu đầu ra để ngăn chặn các tấn công như Cross-Site Scripting (XSS) mà có thể lợi dụng quyền truy cập của quản trị.
6. ***Tự Động Hóa và Quản Lý Quy trình***: Tự động hóa việc cài đặt và triển khai, giảm thiểu sự can thiệp của con người vào hệ thống. Tích hợp quản lý quy trình và thực hiện các bước kiểm tra an toàn.

7. ***Cập Nhật Hệ Thống và Phần Mềm***: theo dõi và cập nhật các phiên bản mới nhất nhằm giảm thiểu các lỗi phần mềm.