**KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)**

**Môn: An toàn thông tin**

**Đề bài: Lần 1**

1. *(3 điểm)* Trình bày về các lỗ hổng phổ biến và giải pháp để đảm bảo an toàn cho Hệ điều hành?
2. *(4 điểm)* Trình bày các nguyên tắc để đảm bảo an toàn cho ứng dụng?

Bài làm:

1. **Các lỗ hổng phổ biến:**

* Lỗ Hổng Zero-Day: các nhà phát triển không có thời gian để khắc phục và không có bản vá nào được phát hành để vá lỗ hổng.
* Buffter Overflow : Tràn bộ đệm, có thể gây ra một ngoại lệ truy nhập bộ nhớ máy tính và chương trình bị kết thúc, hoặc khi người dùng cố tình phá hoại, có thể lợi dụng lỗi này để phá vỡ an ninh hệ thống.
* OS Command Injection (hay còn được gọi là shell injection) là một lỗ hổng bảo mật web cho phép kẻ tấn công thực thi các lệnh hệ điều hành (OS) tùy ý trên máy chủ đang chạy service nào đó. Kẻ tấn công có thể tận dụng lỗ hổng này để khai thác, lấy thông tin, chuyển cuộc tấn công sang hệ thống khác bên trong tổ chức
* SQL Injection: là các lổ hổng thông qua các câu truy vấn SQL, có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update, v.v. trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy
* Uncontrolled Format String: được sử dụng trong nhiều ngôn ngữ lập trình để chèn giá trị vào một chuỗi văn bản. Trong một số trường hợp, cơ chế này có thể bị lạm dụng để thực hiện các cuộc tấn công tràn bộ đệm, trích xuất thông tin hoặc thực thi mã tùy ý.

**Giải pháp đảm bảo an toàn cho hệ điều hành:**

* Dựa theo mô hình CIA (tính bảo mật- tính toàn vẹn- tính sẵn sàng): trên lý thuyết là vậy.
* Giáo dục người dùng, đào tạo nâng cao nhận thức
* Installing and patching: kiểm tra và cài đặt các bản vá mới của hệ điều hành
* Thêm một số cơ chế bảo mật khác: Anti-virus, host-based Firewall, IDS/IPS, application white-listing,..
* Test the system security:

+ Chạy một số test cases cố gắng phá vỡ bảo mật

+ Đảm bảo các bước cấu hình bảo mật trước đó được triển khai chính xác

+ Xác định bất kỳ lỗ hổng có thể có

* Application Security: chú ý đến một số ứng dụng mà chúng ta cài thêm vô

+ Cài đúng cách

+ Mã hóa dữ liệu trong quá trình lưu trữ và vận chuyển

+ Giới hạn đặc quyền đối với user

+ Các ứng dụng có thể cung cấp backdoors nếu không được định cấu hình đúng cách

* Bảo trì an ninh (Security Maintenance): phải duy trì liên tục quy trình bảo mật

+ Giám sát và phân tích thông tin

+ Thường xuyên backups

+ Recovering from security compromises

+ Kiểm tra thường xuyên

+ Cập nhật và sửa đổi các phần mềm quan trọng

* Cài đặt công cụ quét để tìm kiếm các lỗ hổng hệ điều hành và các đoạn mã chương trình không được bảo vệ, phát hiện và cập nhật các phần mềm và plug-in đã lỗi thời để bảo vệ máy tính khỏi các cuộc tấn công độc hại.
* Network protection
* Malware protection
* Virtualization security

1. **Các nguyên tắc để đảm bảo an toàn cho ứng dụng:**

* Nguyên tắc đặc quyền tối thiểu: Nguyên tắc này có thể áp dụng cho cả việc bảo vệ môi trường vật lý cũng như bảo đảm an toàn cho các hệ thống mạng và máy chủ. Nguyên tắc đặc quyền tối thiểu quy định rằng một chủ thể (có thể là người dùng, ứng dụng hoặc tiến trình) chỉ nên có các quyền và đặc quyền cần thiết để thực hiện nhiệm vụ của mình mà không nên được cấp các quyền bổ sung không cần thiết. Việc hạn chế các đặc quyền của đối tượng giới hạn mức độ tổn hại có thể gây ra đối với hệ thống.
* Nguyên tắc phân quyền: là cơ chế sử dụng để cấp quyền truy cập tài nguyên hệ thống dựa trên nhiều yếu tố khác nhau của đối tượng
* Nguyên tắc defense-in-depth: nguyên tắc được đặc trưng bởi việc sử dụng nhiều cơ chế phòng thủ khác nhau theo nhiều lớp. Khi một lỗ hổng bị khai thác ở các lớp phía trước, các cơ chế bảo vệ khác ở các lớp phía sau vẫn tồn tại và do đó hệ thống trở lên mạnh và khó bị tấn công hơn.
* Nguyên tắc đóng gói: Nguyên tắc này được thực hiện bằng cách đóng gói một tập hợp các thủ tục và đối tượng dữ liệu trong một miền của chính nó để cấu trúc bên trong của đối tượng dữ liệu chỉ có thể truy cập được đối với các thủ tục hoặc hàm con của hệ thống được bảo vệ và các thủ tục chỉ có thể được gọi tại các điểm được chỉ định.
* Nguyên tắc tường minh: đảm bảo rằng một chương trình hoặc giao diện người dùng phải luôn phản hồi một cách thân thiện, dễ sử dụng và rõ ràng nhất cho người dùng.
* Nguyên tắc mềm dẻo hệ thống: tính mềm dẻo hệ thống sẽ giúp cho việc nâng cấp hệ thống dễ dàng mà không phải thay thế mới toàn bộ máy móc thiết bị của hệ thống.
* Để đảm bảo ứng dụng an toàn cần thực hiện một số biện pháp sau:

+ Đào tạo đội ngũ thông thạo (train, hire, orther)

+ Xây dựng nhiều lớp bảo vệ cho hệ thống

+ xây dựng chính sách bảo mật, quy trình hoạt động cho hệ thống(đối với các doanh nghiệp, tuân thủ theo chuẩn ISO 27001/27002,…)

+ Đào tạo nâng cao nhận thức

***Hướng dẫn nộp bài:***

* Đặt tên file: ***MSSV*\_*HoTen*\_Ktra\_PartI** (file word hoặc pdf)
* Nộp bài trên hệ thống utex.hcmute.edu.vn mục **Bài KT tự luận**
* Thời gian nộp bài: trước **18:30**  ngày 13/10/2022

**KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)**

**Môn: An toàn thông tin**

**Đề bài: Lần 2**

1. *( 3,0 điểm)*
   1. Trình bày sự khác nhau giữa IDS và IPS?

* IDS (Intrusion Detection Systems) - Hệ thống phát hiện xâm nhập: Có khả năng phát hiện xâm nhập và cảnh báo, nhưng không có khả năng ngăn chặn lại các xâm nhập.
* IPS (Intrusion Prevention System) là Hệ thống Ngăn chặn Xâm nhập: có khả năng phát hiện xâm nhập và ngăn chặn sự xâm nhập hoặc tấn công đó.
  1. Trình bày về firewall và firewall rules?

**FireWall**

* Một phần của hệ thống máy tính hoặc mạng được thiết kế để ngăn chặn truy cập trái phép đi qua nó.
* Chia mạng ra thành nhiều phần: inside – outside (trusted and untrusted)
* Phân biệt mạng thành các khu vực có độ bảo mật khác nhau
* Chức năng chính là lọc dữ liệu (filtering) dựa vào các rule mà người ta đã thiết lập trước đó để chống lại các truy cập bất hợp pháp hay các tấn công.

Yêu cầu của Firewall

* Tất cả truy cập giữa các vùng tin cậy phải vượt qua tường lửa.
* Chỉ truy cập được phép, như được xác định bởi chính sách bảo mật, mới được phép đi qua.
* Bản thân Firewall phải miễn nhiễm với sự xâm nhập, nghĩa là sử dụng một hardened system với Hệ điều hành được bảo mật.

Policy

* User control: Kiểm soát quyền truy cập của người dùng
* Service control: Kiểm soát các dịch vụ, giao thức
* Direction control: Kiểm soát hướng (inbound/ outbound)

Firewall actions

* Permit/ Allow/ accepted: Cho phép truy cập
* Deny/ Drop/ Rejected: Từ chối truy cập

Type firewall

Phân loại dựa vào cách xử lý:

* Packet Filter Firewall/ Stateless Firewall / Per packet: Xử lý từng gói riêng lẻ
* Stateful Firewall/ Per flow Firewall: Xử lý một lúc nhiều gói có mối liên quan với nhau
* Application/Proxy Firewall

Phân loại dựa vào vị trí:

* External Firewall: bên ngoài
* Internal Firewall: Nội bộ

**Firewall Rules**

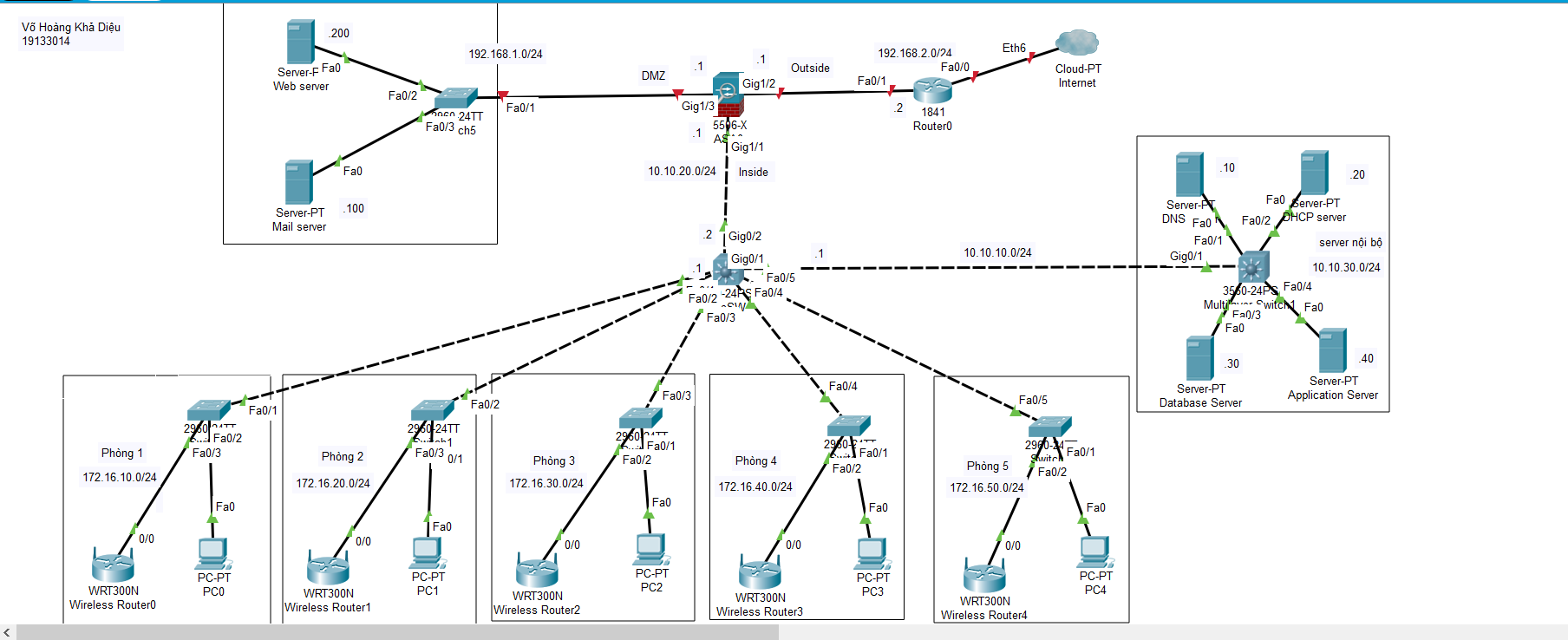
* **Cấu trúc:** Rule\_name, action, source, destination
* Có tính thứ tự
* Xác định lưu lượng mà tường lửa của bạn cho phép và những gì bị chặn.
* Kiểm tra thông tin điều khiển trong các gói riêng lẻ và chặn hoặc cho phép chúng theo các tiêu chí mà bạn xác định.
* Kiểm soát cách tường lửa bảo vệ mạng của bạn khỏi các chương trình độc hại và truy cập trái phép.
* Quản lý các quy tắc tường lửa trên các thiết bị của bạn và trong toàn bộ mạng của bạn là rất quan trọng đối với an ninh mạng.

Với các Firewall Rules, có thể triển khai các chính sách và hành động để thực thi các biện pháp kiểm soát bảo mật và ưu tiên lưu lượng truy cập

1. *(3,0 điểm)* Vẽ sơ đồ logic cho một công ty có các đặc điểm sau:

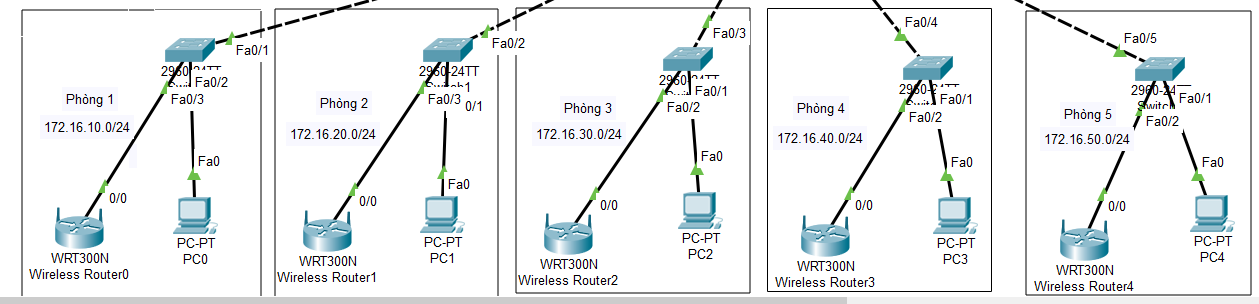
* 5 phòng ban
* 01 khu vực đặt các server nội bộ bên trong như: DNS server, DHCP server, Database Server, Application Server
* 01 khu vực đặt các server public gồm: Web server, Mail server
* Công ty có triển khai mạng WiFi

Sử dụng các thiết bị mạng đã biết: Router, Switch, Firewall, IDS/IPS,… thiết kế cho hệ thống mạng trên.

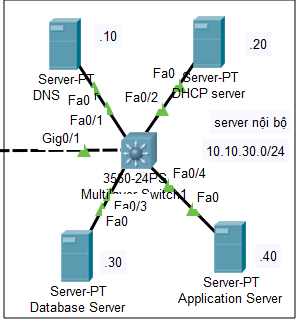


1. *(4,0 điểm)* Dựa vào sơ đồ ở câu 2, SV thực hiện các yêu cầu sau:
   1. Đặt địa chỉ IP cho các khu vực trong sơ đồ đã vẽ (SV có thể ghi địa chỉ trực tiếp trên sơ đồ mạng ở câu 2).

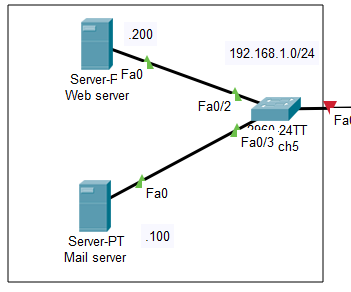
* Địa chỉ IP Cho các phòng ban lần lượt là: **172.16.x.0/24(x lần lượt là 10, 20, 30, 40, 50)**



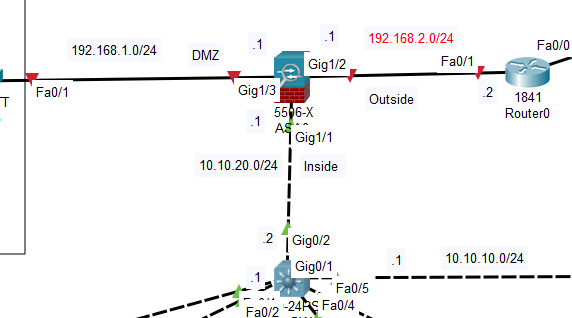
* Khu vực Server nội bộ có ip là **10.10.30.0/24**



* Khu vực server public có ip **192.168.1.0/24**



* Địa chỉ IP cho các đường truyền kết nối: **10.10.10.0/24**, **10.10.20.0/24**, **192.168.1.0/24**, **192.168.2.0/24**



* 1. Mô tả ngắn gọn cách thiết kế cho công ty trên, thiết kế như vậy mang lại các lợi ích gì ?
* Thiết kế mạng theo mô hình sao có tốc độ nhan. Khi xảy ra xự cố cáp mạng bị đứt thì thông thường chỉ làm hỏng kết nối của một máy, các máy khác vẫn hoạt động được. Khi có lỗi mạng, ta dễ dàng kiểm tra sửa chữa.
* Tất cả các truy cập bên ngoài khi muốn truy cập vào hệ thống phải thông qua Firewall, từ đó có thể quản lý được lưu lượng truy cập nhằm tránh bị tấn công Dos, Ddos
* FireWall chia hệ thống thành nhiều khu vực riêng biệt: Inside, DMZ, Outside. Mỗi khu vực có mức độ bảo mật khác nhau.
* Cụm DMZ gồm Mail Server và Web Server có thể liên kết với internet bên ngoài nhưng vẫn phải qua Firewall và hệ thống IPS để đảm bảo an toàn.
* Khu vực Inside cũng được tách riêng biệt với nhau để dễ quản lý
  1. Phân tích một số giải pháp để bảo vệ và nâng cao tính sẵn sàng của Web server và Email server trong thiết kế trên.
* Cài đặt chứng chỉ SSL là cách bảo mật website được nhiều người biết đến. SSL bảo mật dựa theo cơ chế mã hóa thông tin giữa trình duyệt client và server, giúp thông tin được bảo vệ.
* Cập nhật web application: Cập nhật các phần mềm ứng dụng giúp sửa lại các lỗ hổng, lỗi của phiên bản trước. Đây cũng là một trong những biện pháp đơn giản nhưng hữu hiệu để tránh khỏi sự tấn công của các hacker.
* Web application firewall (WAF)- tường lửa ứng dụng web: Tường lửa ứng dụng web có chức năng tự động phân tích các lỗ hổng có thể bị xâm nhập, chống lại các code độc, sự tấn công của các hacker hoặc virus.
* Sử dụng VPN (Virtual Private Network): mã hóa dữ liệu, xác thực danh tính người dùng, quản lý phiên truy cập của người dùng
* Sử dụng chữ ký số (Digital Signature): nhằm mục đích xác định người chủ của dữ liệu đó.

***Hướng dẫn nộp bài:***

* Đặt tên file: ***MSSV*\_*HoTen*\_Ktra\_PartII** (file word hoặc pdf)
* Nộp bài trên hệ thống utex.hcmute.edu.vn mục **Bài KT tự luận**
* Thời gian nộp bài: trước **19:15**  ngày 24/11/2021