KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)

Môn: An toàn thông tin

Đề bài:

1. *(3,0 điểm)* Tấn công từ chối dịch vụ là gì? Giải pháp hạn chế kiểu tấn công này?
2. *(3,0 điểm)* Vẽ sơ đồ logic cho một công ty có các đặc điểm sau:

- 6 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.

3. *(4,0 điểm)* Dựa vào sơ đồ mạng ở câu 2, SV thực hiện các yêu cầu sau:
    a. 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).
    b. Mô tả ngắn gọn cách thiết kế cho công ty trên, các thiết kế như vậy mang lại các lợi ích gì ?
    c. Phân tích một số giải pháp có thể sử dụng để bảo vệ hệ thống mạng nội bộ (khu vực mạng LAN – hay gọi là khu vực INSIDE) trong thiết kế trên.

Hướng dẫn nộp bài:

- Đặt tên file: ***MSSV_HoTen*_Ktra_PartII** (file word hoặc pdf)
- Nộp bài trên hệ thống mục **Bài KT tự luận**

Bài làm

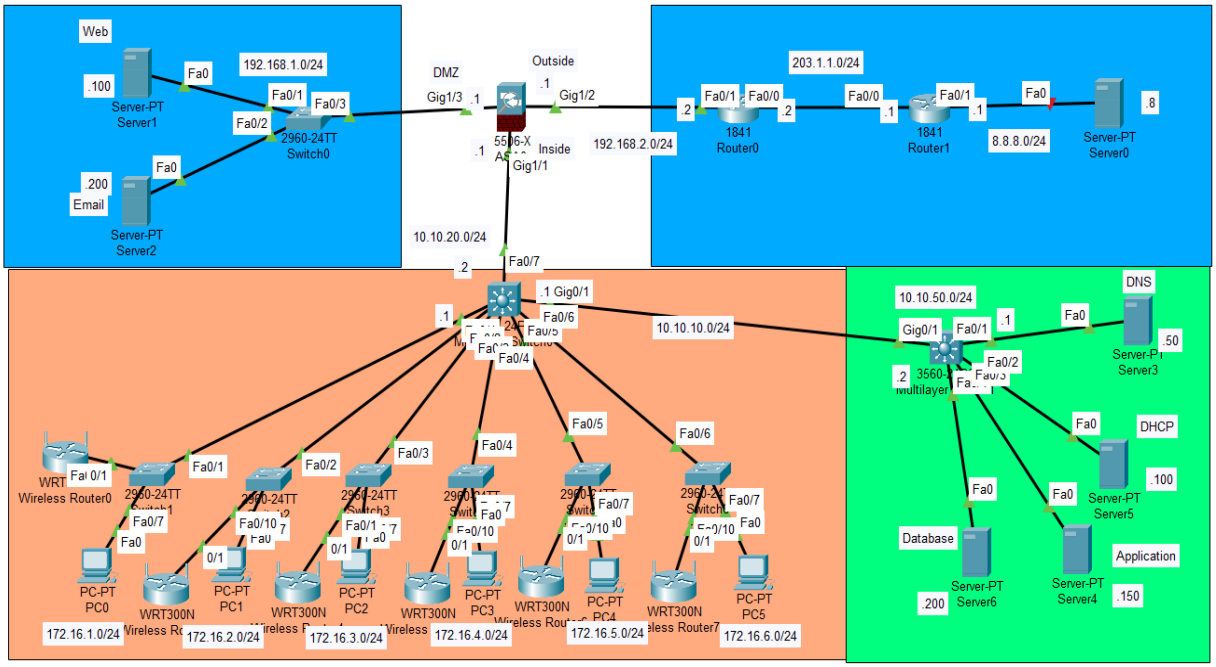
Câu 1:

- Tấn công từ chối dịch vụ (DoS/DDoS) là một kiểu tấn công ác ý của một người hay nhiều người làm cho để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, làm gián đoạn dịch vụ internet, bằng cách làm quá tải tài nguyên của hệ thống, phá vỡ lượng truy cập bình thường của máy chủ. Thủ phạm tấn công từ chối dịch vụ thường nhắm vào các trang

mạng hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

- Các giải pháp hạn chế tấn công từ chối dịch vụ:
  + Sử dụng tường lửa (Firewall): đặt firewall giữa internet và server để bảo vệ server
  + Tăng cường phần cứng và băng thông: cung cấp lưu lượng truy cập cao gấp 10 lần bình thường khi thiết kế mạng
  + Sử dụng mạng Anycast để phân tán lưu lượng tấn công
  + Giám sát trang web từ xa qua các nhà cung cấp dịch vụ bên thứ ba

Câu 2:



Câu 3:

b) - Cách thiết kế : Cho các puplic server vào khu vực DMZ và các server nội bộ vào trong Inside ngăn cách các khu vực này bằng Firewall, các phòng ban đặt mỗi phòng một switch và một wifi router để kết nối wifi. Đặt một ISP giữa router và internet

- Thiết kết công ty như sơ đồ trên giúp công ty bảo vệ được các puplic server trước các cuộc tấn công nhờ external firewall đóng ai trò như một proxy ngược và nhờ

dịch vụ ISP có thể kịp thời phát hiện những vụ tấn công điển hình là tấn công từ chối dịch vụ DoS. Tóm lại là giúp bảo vệ mạng tốt hơn

c) Một số cách để bảo vệ mạng nội bộ là sử dụng IDS và IPS vào thiết kế trên dùng IPS và giữa tường lửa và mạng nội bộ để khi traffic đi vào mạng nội bộ bị giám sát và kịp thời báo cho firewall. IDS gắn trên switch layer vào inside để copy traffic thông báo cho firewall