TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO

XÂY DỰNG CHIẾN LƯỢC BẢO MẬT CHO HỆ THỐNG THÔNG TIN DOANH NGHIỆP

TRẦN NGỌC VINH – 21DH113413

LÊ THÀNH ÂN – 21DH112304

NGUYỄN HOÀNG PHÚC – 21DH114014

TRANG MINH HIỂN – 21DH110549

MÔN HỌC

QUẢN TRỊ HỆ THỐNG BẢO MẬT

HƯỚNG DẪN KHOA HỌC: NGUYỄN ANH VŨ

Sản phẩm này chỉ dùng cho mục đích giáo dục

Ngày báo cáo: 27/03/2024

Tiêu chí đánh giá

- *Giá trị thực tiễn (2đ)* :
- *Khả năng đồng bộ (3đ)* :
- *Quy mô triển khai (3đ)* :
- *Kỹ năng vấn đáp (2đ)* :

Tổng điểm

NHẬN XÉT CỦA GIẢNG VIÊN

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

LỜI MỞ ĐẦU

Ngày nay, việc ứng dụng công nghệ thông tin đã trở nên phổ biến trong hầu hết mọi cơ quan, doanh nghiệp, trường học đặc biệt là việc áp dụng các giải pháp tin học trong công tác quản lý hoặc để xây dựng những hệ thống phục vụ cho một mục đích nào đó. Với sự phát triển vượt bậc của công nghệ ngày một được đưa vào đời sống của chúng ta nhiều hơn, có thể nói rằng hầu hết mọi công việc, tác vụ hoặc giải trí đã và đang ngày một được gói gọn trong những thiết bị sử dụng hằng ngày.

Công nghệ thông tin trở thành một ngành học, một lĩnh vực không thể thiếu để áp dụng vào nhiều lĩnh vực khác liên quan đến mọi ngành nghề, giúp cho đời sống của chúng ta ngày một dễ dàng, tiện lợi và nhanh chóng hơn. Tuy rằng công việc tự học của học sinh, sinh viên trong lĩnh vực này là vô cùng quan trọng nhưng như thế vẫn là chưa đủ. Việc kết hợp yếu tố giảng dạy từ những giáo viên và người khác thì tốc độ tiếp tục và áp dụng kiến thức của chúng ta sẽ được tăng lên rất nhiều, giúp chúng ta có tính tư duy, vận dụng, tính sáng tạo cũng như kế thừa để phát huy những ưu điểm của người giảng dạy. Bởi vì những yếu tố ấy, để bắt kịp với tốc độ phát triển của xã hôi, những kiến thức có được nhờ việc đi học đầy đủ trên giảng đường là vô cùng quan trọng đối với chúng em.

LỜI CẢM ƠN

Trong thời gian làm đồ án bộ môn Quản trị hệ thống bảo mật, em đã nhận được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, gia đình và bạn bè.

Em xin gửi lời cảm ơn chân thành cảm ơn thầy Nguyễn Anh Vũ - giảng viên Bộ môn Quản trị hệ thống bảo mật của trường đại học Ngoại Ngữ - Tin Học (HUFLIT) người đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình làm khoá luận.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường nói chung, các thầy cô của chuyên ngành An Ninh Mạng thuộc Công Nghệ Thông Tin nói riêng đã dạy dỗ cho em kiến thức về các môn đại cương cũng như các môn chuyên ngành, giúp em có được cơ sở lý thuyết vững vàng và tạo điều kiện giúp đỡ em trong suốt quá trình học tập.

Cuối cùng, em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, giúp đỡ, động viên em trong suốt quá trình học tập và hoàn thành khoá luận tốt nghiệp.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế của một học viên, luận văn này không thể tránh được những thiếu sót. Em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô để tôi có điều kiện bổ sung, nâng cao ý thức của mình, phục vụ tốt hơn công tác thực tế sau này.

MỤC LỤC

DANH MỤC HÌNH ẢNH

CHƯƠNG I: TỔNG QUAN VỀ BẢO MẬT

1. Bảo mật thông tin là gì ?

Bảo mật thông tin (Information Security) không đơn thuần là bảo vệ thông tin của cá nhân người dùng mà còn là một loạt các chiến lược nhằm ngăn chặn những truy cập, hành vi trái phép liên quan tới tài sản, dữ liệu, thông tin riêng của tổ chức/ cá nhân.

2. Bảo mật thông tin doanh nghiệp là gì ?

An toàn và bảo mật thông tin đặc biệt quan trọng trong các doanh nghiệp, tổ chức vì nó ảnh hưởng rất nhiều tới các hoạt động của các doanh nghiệp và tổ chức. Bảo mật thông tin trong doanh nghiệp bao gồm tất cả các hoạt động như :

- Phòng ngừa hiện tượng đánh cắp, sao chép dữ liệu nội bộ
- Ngăn chặn tin tặc đánh cắp danh tính, cài các phần mềm độc hại vào hệ thống doanh nghiệp
- Đảm bảo những trao đổi thông tin dữ liệu, giao dịch, kinh doanh online ở trạng thái an toàn nhất
- Mọi thông tin liên quan tới hoạt động, giao dịch, tài chính, nhân sự, khách hàng cần được giữ bí mật tuyệt đối bởi các phòng ban có liên quan, …

3. Vấn đề bảo mật thông tin hiện nay tại Việt Nam

Công nghệ ngày càng phát triển, các nhà lập trình ứng dụng và chuyên viên bảo vệ thông tin đang có xu hướng tiếp cận công nghệ mới để nâng cấp "hàng rào bảo vệ" cho các cá nhân/ tổ chức.

Tại các hệ thống lớn, thường thì trong hoặc sau một sự cố bảo mật, đội ngũ IT Security có thể đưa ra kế hoạch ứng phó sự cố cũng như thiết lập các công cụ quản lý rủi ro để lấy lại quyền kiểm soát tình hình.

Nhưng dường như chỉ thế thôi là chưa đủ, số lượng hệ thống mới trên thị trường tăng nhanh trong khi cơ sở hạ tầng tại Việt Nam không đáp ứng đủ. Đó chính là thách thức mà chúng ta đang phải đối mặt.

4. Các loại bảo mật thông tin :

Tuỳ theo nguyên tắc phân loại mà bảo mật thông tin được phân chia thành các loại khác nhau. Nếu chia theo lĩnh vực thì chúng ta có bảo mật thông tin cá nhân, bảo mật thông tin doanh nghiệp, bảo mật ứng dụng, bảo mật hệ thống, … Còn nếu chia theo hình thức bảo mật thì ta có

- Bảo mật về mặt vật lý (Physical Security) : Nếu bạn đã hiểu bảo mật thông tin là gì thì sẽ rất dễ nhận ra các hình thức bảo mật vật lý. Đó là việc bảo vệ thông tin khỏi các yếu tố do thiên nhiên/ con người/ hành vi vật lý thực hiện như đột nhập trái phép, trộm cắp, đánh đập cũng như các yếu tố tự nhiên như mất điện, mưa, bụi, lửa, …
- Bảo mật về mặt kỹ thuật : Là việc ứng dụng khoa học kỹ thuật vào để bảo mật hệ thống như dựng "tường lửa", cài đặt phần mềm chống virus, thiết lập hệ thống bảo mật dữ liệu, hệ thống phân quyền, …

5. Mục tiêu của việc bảo mật thông tin

Có 4 mục tiêu mà bất cứ hệ thống an toàn thông tin nào cũng phải nắm được, đó chính là :

- Ngăn chặn : Thiết lập các biện pháp để ngăn chặn sự tấn công từ tác nhân vật lý, các tác nhân kỹ thuật hoặc các hành vi vi phạm chính sách bảo mật.
- Phát hiện : Nhanh chóng phát hiện ra các hành vi vi phạm ảnh hưởng tới cá nhân/ hệ thống.
- Phục hồi : Sửa chữa, khắc phục hậu quả kịp thời để đảm bảo mọi thứ hoạt động bình thường. Bên cạnh đó, bạn cũng cần đánh giá được hành vi vi phạm để không bị lặp lại trong tương lai.
- Hoạt động : Và mục tiêu lớn nhất của bảo mật thông tin là gì? Đó chính là đảm bảo hệ thống, cá nhân luôn ở trạng thái tốt nhất, không thể bị ảnh hưởng quá nhiều bởi các phần mềm độc hại.

CHƯƠNG II : TỔNG QUAN VỀ MÔ HÌNH THIẾT KẾ VÀ TRIỂN KHAI

1. MÔ HÌNH :

1. Giới thiệu về doanh nghiệp :

Tên của công ty : VPHA

Lĩnh vực : kinh doanh trang thiết bị điện tử về máy tính tư nhân

Quy mô hoạt động : tòa nhà cấp 3 (bao gồm 1 trệt và 1 lầu) ; tầng trệt có 1 phòng máy server và 1 phòng máy nhân viên (client), tầng 1 có 1 phòng máy nhân viên

Tổng số chi nhánh : 1

Tổ chức phòng ban : phòng nhân sự, phòng kinh doanh tiếp thị, phòng tư vấn và dịch vụ khách hàng, phòng máy server

Vai trò :

- Phòng nhân sự : Quản lý nhân sự, tuyển dụng, đào tạo, giải quyết xung đột lao động, …
- Phòng kinh doanh tiếp thị : Phát triển chiến lược kinh doanh, quảng cáo, bán hàng, tìm hiểu thị trường, tìm kiếm khách hàng
- Phòng tư vấn và dịch vụ khách hàng : Tư vấn sản phẩm, hỗ trợ và giải quyết vấn đề cho khách hàng khi có yêu cầu.
- Phòng server : Quản lý và vận hành các máy tính trong hệ thống công ty, bảo mật dữ liệu, lưu trữ thông tin.

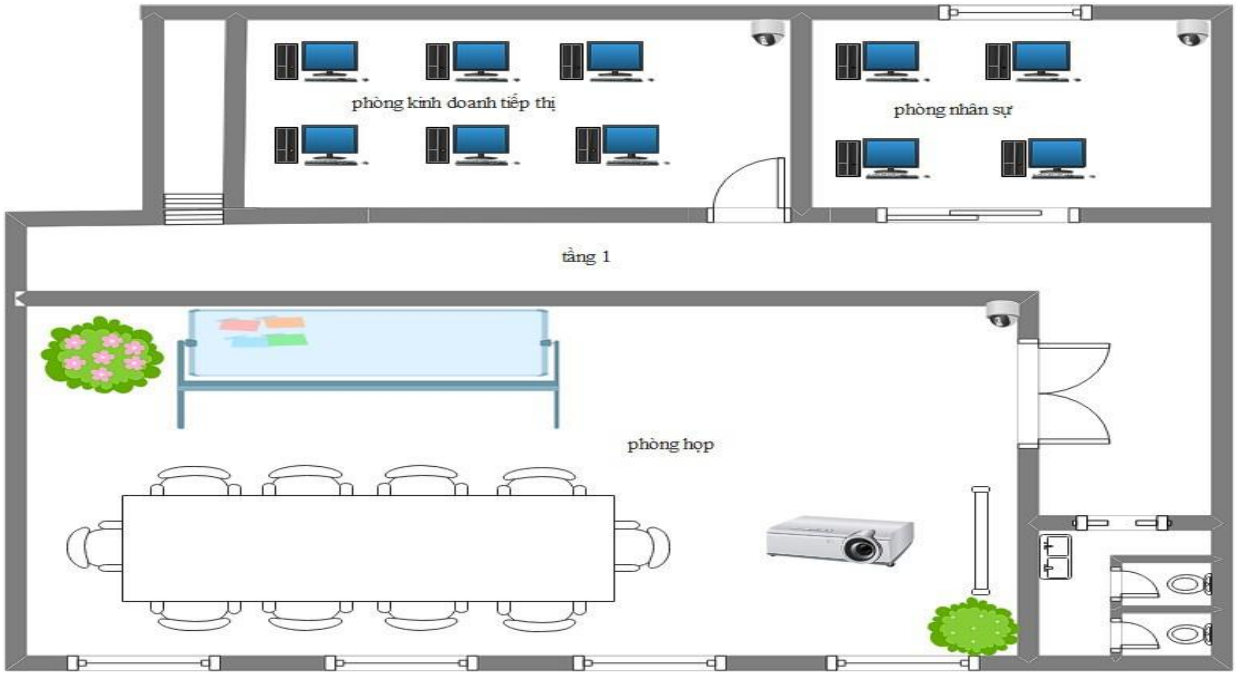
2. Thiết kế hệ thống :

IP table :

STT	DEVICE	IP	SUBNET MASK	DEFAULT GATEWAY	NOTE
1	KERIO CONTROL (Firewall)	WAN: DHCP Ethernet: 118.67.34.4	255.255.255.224		
2	SERVER CHÍNH	118.67.34.6	255.255.255.224	118.67.34.4	
3	SERVER Phụ (Sever backup)	118.67.34.7	255.255.255.224	118.67.34.4	
4	TẦNG 1: 10 PC cấu hình tương đối	118.67.34.8 -> 118.67.34.30	255.255.255.224	118.67.34.4	
5	TẦNG 2: 10 PC cấu hình tương đối		255.255.255.224	118.67.34.4	

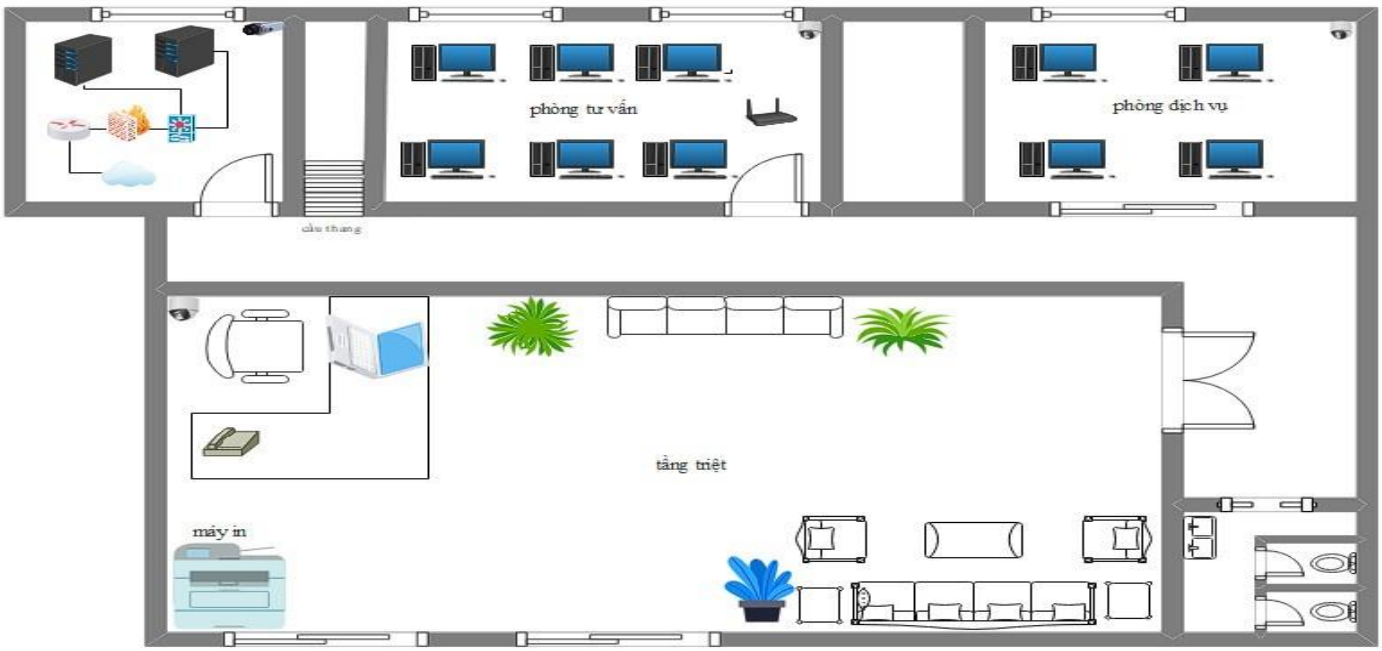
Sơ đồ vật lý :

Tầng 1 :



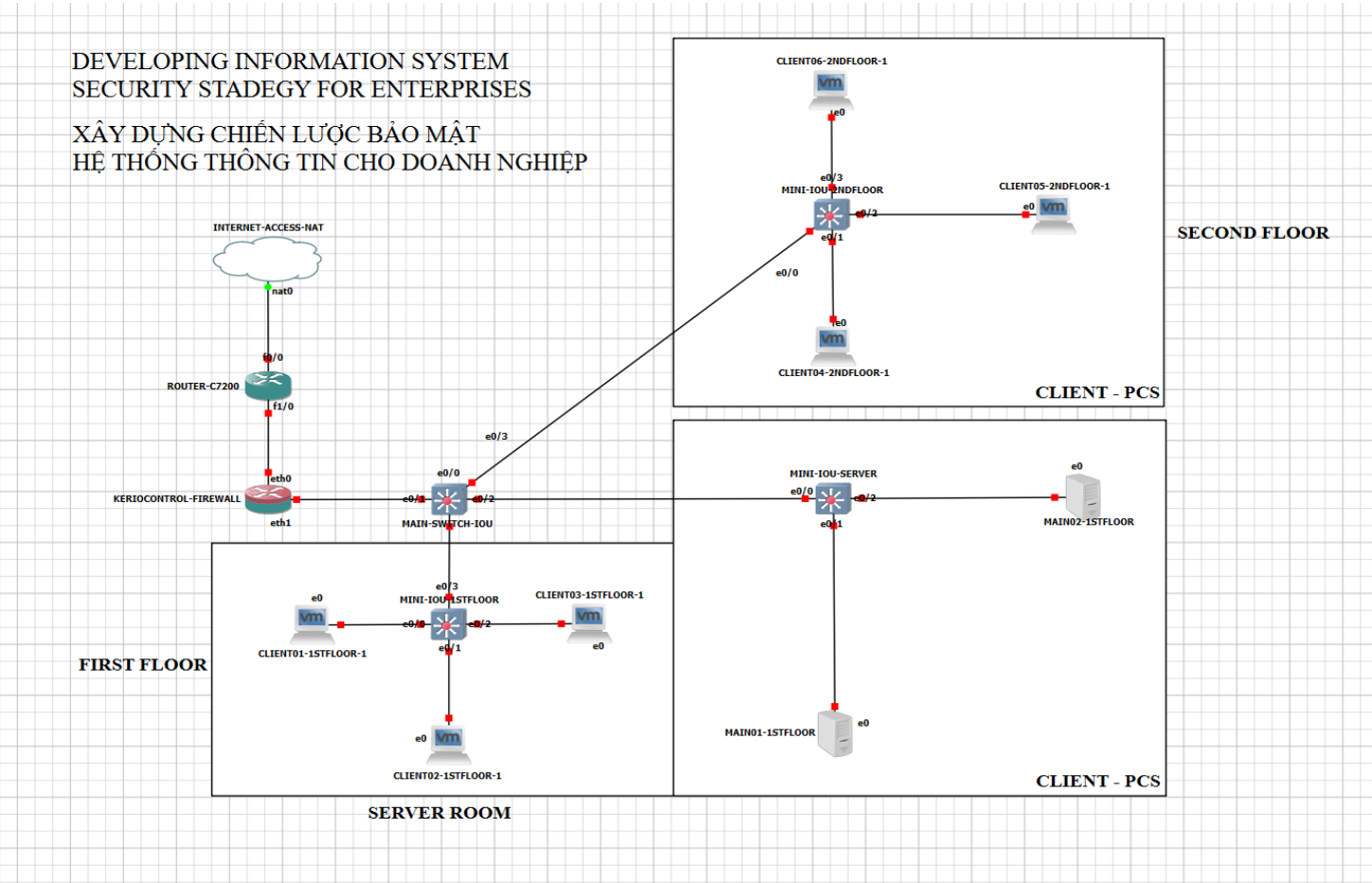
Hình. 1.Sơ đồ vật lý tầng 1

Tầng 2 :



Hình. 2.Sơ đồ vật lý tầng 2

Sơ đồ logic :



Hình. 3 Sơ đồ logic của công ty

3. CHIẾN LƯỢC BẢO MẬT VÀ TRIỂN KHAI :

3.1 Các dạng tấn công bảo mật thông tin đối với doanh nghiệp :

Để đưa ra các biện pháp bảo mật cần thiết cho một hệ thống mạng doanh nghiệp, cần tìm hiểu những cách tấn công của tin tặc. Tin tặc thường tấn công dữ liệu doanh nghiệp thông qua nhiều hình thức và sau đây là những mối đe dọa tới an toàn thông tin doanh nghiệp :

Phishing (Tấn công giả mạo) là hình thức tấn công mạng mà kẻ tấn công giả mạo thành một đơn vị uy tín để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng.

Khai thác lỗ hổng bảo mật trong các ứng dụng, phần mềm

Lỗ hổng bảo mật (vulnerability) là một khái niệm phổ biến trong giới an toàn thông tin. Có rất nhiều định nghĩa khác nhau về lỗ hổng, nhưng tất cả đều có điểm chung là ám chỉ một điểm yếu (kỹ thuật hoặc phi kỹ thuật) của một phần mềm, phần cứng, giao thức, hay một hệ thống thông tin.

Dưới đây là một số định nghĩa về lỗ hổng bảo mật :

- Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) : Điểm yếu trong hệ thống thông tin, quy trình bảo mật hệ thống, kiểm soát nội bộ hoặc công tác triển khai có thể bị khai thác bởi tác nhân gây hại.
- ISO 27005 : Điểm yếu của một tài sản hoặc nhóm tài sản có thể bị khai thác bởi một hoặc nhiều mối đe dọa trên mạng, trong đó tài sản là bất cứ thứ gì có giá trị đối với tổ chức, hoạt động kinh doanh của tổ chức và tính liên tục của những hoạt động đó, bao gồm các tài nguyên thông tin hỗ trợ sứ mệnh của tổ chức.
- IETF RFC 4949 : Một lỗ hổng hoặc điểm yếu trong thiết kế, triển khai hoặc vận hành và quản lý của hệ thống có thể bị khai thác để vi phạm chính sách bảo mật của hệ thống.
- ENISA : Sự tồn tại của một điểm yếu, thiết kế hoặc lỗi triển khai có thể dẫn đến một sự cố không mong muốn làm tổn hại đến bảo mật của hệ thống máy tính, mạng, ứng dụng hoặc giao thức liên quan.

- The Open Group : Xác suất khả năng của mối đe dọa vượt quá khả năng chống lại mối đe dọa đó.
- Phân tích nhân tố về rủi ro thông tin : Xác suất một tài sản sẽ không thể chống lại hành động của một tác nhân đe dọa.
- ISACA : Một điểm yếu trong thiết kế, triển khai, vận hành hoặc kiểm soát nội bộ.

Tiêm nhiễm (Injection) là một kỹ thuật thường được sử dụng bởi các kẻ tấn công để chèn các đoạn mã độc hại vào hệ thống hoặc ứng dụng mục tiêu thông qua các cơ chế nhập dữ liệu. Đối với các ứng dụng web, injection thường diễn ra khi kẻ tấn công chèn các đoạn mã độc hại vào các trường nhập liệu của biểu mẫu web hoặc các tham số truy vấn của URL. Các loại injection phổ biến bao gồm SQL Injection, XSS (Cross-Site Scripting), LDAP Injection, và Command Injection.

Tấn công mật khẩu là hình thức hacker tìm cách hack mật khẩu và truy cập vào tài khoản của bạn. Vì thế, tấn công mật khẩu còn có tên gọi khác là hack password. Mục đích chính của tấn công mật khẩu chính là truy cập tài khoản và lừa đảo. Một số tài khoản thường xuyên bị hack password là facebook, gmail. Tấn công chuỗi cung ứng

Tấn công hệ thống CRM (Customer Relationship Management) là một loại cuộc tấn công nhằm vào các hệ thống và dữ liệu của các hệ thống CRM, mục đích có thể là lấy thông tin khách hàng quan trọng, gây ra sự cố hoặc hại cho doanh nghiệp.

3.2 Các biện pháp bảo mật

Sau khi tìm hiểu các cách tấn công của tin tặc đối với doanh nghiệp thì sau đây là các giải pháp bảo mật :

Firewall (Tường lửa) : giúp kiểm soát luồng thông tin giữa Intranet và Internet, chúng phát hiện và phán xét những hành vi được truy cập và không được truy cập vào bên trong hệ thống, đảm bảo tối đa sự an toàn thông tin.

Một số chức năng chính của tường lửa bao gồm :

- Ngăn chặn truy cập không ủy quyền : Tường lửa có thể cấu hình để chặn các kết nối đến hoặc từ nguồn không ủy quyền.
- Kiểm soát truy cập dịch vụ : Tường lửa có thể kiểm soát truy cập vào các dịch vụ cụ thể như web, Email, FTP, SSH, …
- Phân loại lưu lượng mạng : Tường lửa có thể phân loại lưu lượng mạng dựa trên các quy tắc được cấu hình trước, ví dụ như địa chỉ IP, cổng, giao thức, …
- Giám sát và báo cáo : Tường lửa thường có khả năng giám sát lưu lượng mạng và tạo ra các báo cáo về các sự kiện bảo mật quan trọng như các cuộc tấn công hoặc các hoạt động đáng ngờ.

Sao lưu và khôi phục dữ liệu : Thực hiện sao lưu và kiểm tra tính đúng đắn, chính xác của một số dữ liệu theo thời gian định kì và đảm bảo có thể khôi phục lại dữ liệu khi xảy ra sự cố

Các chính sách bảo mật : thực hiện và tuân thủ các chính sách bao gồm việc sử dụng dữ liệu, truy cập mạng và xữ lý những dữ liệu cần thiết

Kiểm tra và giám sát hệ thống : thường xuyên kiểm tra và giám sát hệ thống để kịp thời phát hiện và ngăn chặn các hành động đáng ngờ

Cập nhật và sửa lỗi hệ thống : cập nhật theo thời gian định kì và sửa kịp thời các lỗi của hệ thống để ngăn chặn các mối nguy tiềm ẩn

Đào tạo nhân viên : Huấn luyện nhân viên về các nguy cơ bảo mật, cách nhận biết mối đe dọa và các làm việc với các dữ liệu nhạy cảm một cách an toàn nhất có thể

Chứng thực và phân quyền : sử dụng mật khẩu dài và phức tạp, cấp quyền truy cập dữ liệu quan trọng cho một số người có quyền truy cập dữ liệu đó

4.Triển khai và thực hiện sử dụng GNS3 :

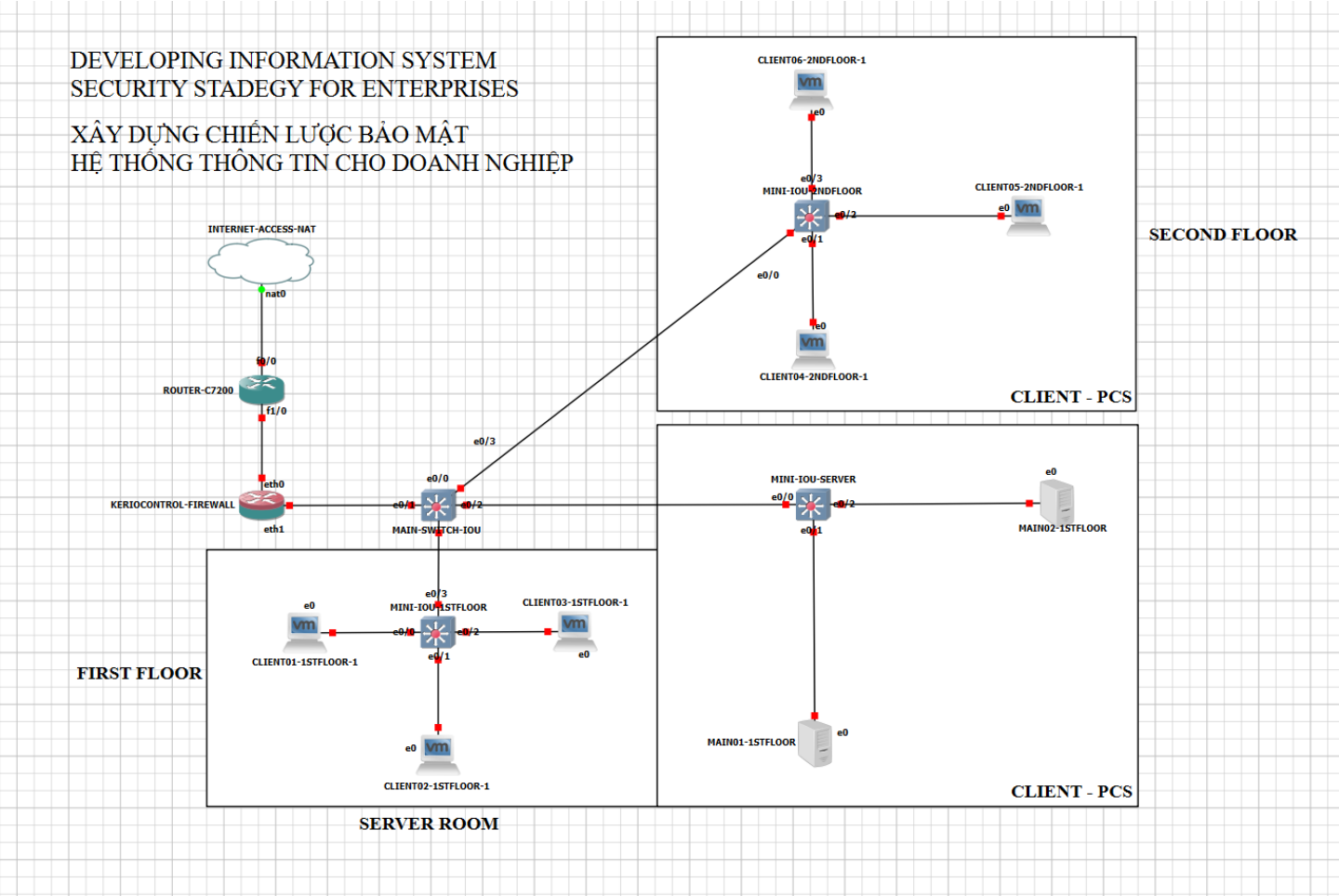
4.1 Cài đặt và mô phỏng trên công cụ GNS3 :

GNS3 là một phần mềm mô phỏng mạng mã nguồn mở được sử dụng phổ biến trong việc thiết kế, mô phỏng và thử nghiệm các mạng máy tính. Tên GNS3 đến từ từ viết tắt của "Graphical Network Simulator-3".

Các tính năng chính của GNS3 bao gồm:

- Mô phỏng mạng: GNS3 cho phép người dùng mô phỏng mạng máy tính bằng cách kết nối các thiết bị mạng ảo như router, switch, firewall và máy tính ảo trên một máy tính vật lý.
- Sử dụng các thiết bị thực tế: GNS3 hỗ trợ tích hợp với các thiết bị mạng thực tế từ các nhà sản xuất như Cisco, Juniper, HP và nhiều hãng khác. Người dùng có thể sử dụng các hình ảnh hệ điều hành và phần cứng của các thiết bị này trong môi trường mô phỏng của GNS3.
- Kiểm tra mạng: GNS3 cung cấp một môi trường an toàn để thử nghiệm các cấu hình mạng và giải pháp mạng mà không cần thiết bị thật, giúp người dùng tối ưu hóa quá trình học tập và nghiên cứu.
- Phân tích và gỡ lỗi mạng: GNS3 cho phép người dùng theo dõi lưu lượng mạng, phân tích hiệu suất và gỡ lỗi mạng bằng cách cung cấp các công cụ quan sát và kiểm tra.
- Hỗ trợ cộng đồng: GNS3 là một dự án mã nguồn mở có một cộng đồng lớn của người dùng và nhà phát triển, cung cấp tài liệu, hướng dẫn và các gói mở rộng để mở rộng khả năng của phần mềm.

4.2 Triển khai mô hình mô phỏng trên GNS3:



Hình. 4 Mô hình mô phỏng trên GNS3

4.3 Tính hiệu quả:

Sử dụng Router CISCO C7200 thay vì các router phổ thông như C3725 để tăng hiệu suất hoạt động, tương thích với nhiều thiết bị kết nối Internet khác nhau.

Có khả năng bảo mật: Tường lửa Firewall Kerio Control (được đặt ở sau CISCO ROUTER C7200), tăng khả năng bảo vệ Router và giảm bớt mức độ phức tạp khi cấu hình mô hình.

Sử dụng Switch CISCO IOU L2 làm Switch tổng và Switch con để chia đường truyền mạng cho các phòng máy, cấu hình các cổng VLAN để cho phép Internet hoạt động.

Sử dụng mô hình máy chủ và máy khách (server – client) để kiểm soát hoạt động nội bộ và phân tích, đánh giá hiệu quả làm việc.

CHƯƠNG III: HƯỚNG DẪN CÀI ĐẶT

1. GNS3:

Tạo một topology và thêm vào các images của các thiết bị mô phỏng mô hình mạng cần thiết:

CISCO ROUTER C7200

SWITCH CISCO IOU L2 15.1

KERIO CONTROL – FIREWALL 9.3.0

Máy ảo từ VMWare: Windows 10 x 64bit, Windows Server 2019 (Desktop Experience).

2. CISCO ROUTER C7200:

Cấu hình CISCO ROUTER C7200 (FastEthernet0/0 kết nối với Internet; FastEthernet1/0 kết nối với KerioControl):

FastEthernet0/0 được cấu hình với địa chỉ IP ngẫu nhiên (DHCP) được lấy từ Mac Address của máy tính thật, overload port.

FastEthernet1/0 được cấu hình với địa chỉ IP tĩnh là 200.200.5.1.

3. SWITCH IOU L2 15.1:

Cấu hình SWITCH CISCO IOU L2 15.1 như sau:

Switch tổng được cấu hình để các cổng từ Ethernet0/0 – 3 có khả năng kết nối và access VLAN 1.

Switch con được cấu hình theo thứ tự phòng máy Server, phòng PC1, phòng PC2 để các cổng từ Ethernet0/0 – 3 có khả năng kết nối và access các VLAN 10, 20, 30.

4. KERIO CONTROL – FIREWALL:

Tường lửa KERIO CONTROL được đặt password, điều chỉnh DHCP với DNS chính là địa chỉ khi đăng nhập tường lửa dưới dạng Web Login, có AntiVirus được tích hợp sẵn

5. Máy ảo từ VMWare:

Windows Server 2019: được thăng cấp lên Server và sử dụng dịch vụ quản lý Active Directory Users and Computers để quản lý các nhân viên trong công ty và có kiểm soát, bảo mật máy khách

Windows 10 x 64bit: được đăng nhập và gia nhập vào hệ thống máy chủ, được sử dụng các dịch vụ mạng cơ bản như OpenVPN, mail nội bộ của máy chủ,…

Tài liệu tham khảo	Reddit
	Google
	Youtube
	GitHub