Noidungontap Tkanht- Dhcntt 17AB

An toàn thông tin (Trường Đại học Công nghiệp Thành phố Hồ Chí Minh)

NỘI DUNG ÔN TẬP MÔN TRIỂN KHAI AN NINH HỆ THỐNG

Để chuẩn bị tốt cho thi cuối kỳ sắp tới, các em ôn tập vào các nội dung trọng điểm sau (dựa trên các LO - chuẩn đầu ra của môn học):

1) Xác định và giải thích được các mối nguy hiểm với một hệ thống cho trước

Yêu cầu: Cho 1 sơ đồ hệ thống mạng, sinh viên phân tích và xác định được 3 mối nguy hiểm khác nhau. Làm cơ sở cho nội dung 2:

2) Vẽ và giải thích được sơ đồ mạng an toàn cho một tình huống cụ thể (DMZ, Firewall, Digital signature)

Yêu cầu: Sinh viên vẽ và giải thích được sơ đồ mạng đáp ứng an toàn cho các mối hiểm hoạ đã phân tích ở trên

3) Giải thích tóm lược được quy trình tấn công

Kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm thông tin,
phá hủy dữ liệu, phá hủy hệ thống.
5 bước để tấn công vào một hệ thống:

- Thăm dò (Reconnaisance)
- Quét lỗ hổng để tấn công (Scanning)
- Cố gắng lấy quyền truy cập (Gaining access)
- Duy trì kết nối (Maintaining access)
- Xóa dấu vết (Cover his track)

1. Thăm dò:
   Một trong những bước qua trọng để biết những thông tin trên hệ thống mục tiêu. Hacker sử dụng kỹ thuật này để khám phá hệ thống mục tiêu đang chạy trên hệ điều hành nào, có bao nhiêu dịch vụ đang chạy trên các dịch vụ đó, cổng dịch vụ nào đang đóng và cổng nào đang mở, gồm hai loại:

   Passive: Thu thập các thông tin chung như vị trí địa lý, điện thoại, email của các cá nhân, người điều hành trong tổ chức.
   Active: Thu thập các thông tin trực tiếp sát với hệ thống: địa chỉ IP, domain, DNS,… của hệ thống
   Quá trình thăm dò có thể phân làm 7 bước:
   B1-Thu thập thông tin ban đầu
   B2-Xác định phạm vi của mạng
   B3-Kiểm tra host có "sống" không ?
   B4-Khám phá những cổng đã mở
   B5-Nhận diện hệ điều hành
   B6-Liệt kê những dịch vụ dựa trên các cổng đã kiểm tra
   B7-Xây dựng sơ đồ mạng
2. Quét hệ thống:
   Sau khi thăm dò để xác định mục tiêu cần tấn công, quét thăm dò nhằm lấy thông tin đến mục tiêu cần tấn công để có kế hoạch tấn công hợp lý
   Là phương pháp quan trọng mà Attacker thường dùng để tìm hiểu hệ thống

và thu thập các thông tin như địa chỉ IP cụ thể, hệ điều hành, các dịch vụ, port đang mở hay các kiến trúc hệ thống mạng.
Phân loại:
+Port scanning
Xác định một cổng TCP/IP đang mở và có sẵn trong hệ thống.
Quét tỉ mỉ: dò quét tất cả các cổng
Quét nhanh: dò quét các cổng thông dụng
Xem thông tin cổng thông dụng: C:\windows\system32\drivers\etc\service
+Network scanning
Xác định máy chủ đang hoạt động trên mạng để tấn công hoặc đánh giá an ninh mạng
+Vulnerability scanning

3. Chiếm quyền điều khiển:
   Chiếm quyền ở các mức:
   Mức hệ điều hành/ mức ứng dụng
   Mức mạng
   Từ chối dịch vụ

4. Duy trì điều khiển:
   Đến giai đoạn này, Attacker thực hiện:
   Upload/download biến đổi thông tin

5. Xóa dấu vết:
   Lý do: Sau khi bị tấn công thì hệ thống sẽ lưu lại những vết do attacker để lại. Attacker cần xoá chúng đi nhằm tránh bị phát hiện.
   Cách thực hiện: Xóa lịch sử…

Quy trình tấn công là một loạt các bước và hoạt động mà một kẻ tấn công thực hiện để xâm nhập vào một hệ thống hoặc tấn công một mục tiêu. Dưới đây là một tóm tắt về quy trình tấn công thông thường:

4) Giải thích được một số kỹ thuật tấn công và phòng thủ

+Tấn công từ chối dịch vụ
Là kiểu tấn công ngăn không cho những người dùng khác truy cập vào hệ thống
Làm cho hệ thống bị quá tải và không thể hoạt động
DoS: tấn công “one-to-one”
DDoS(distributed denial of service)
Sử dụng các Zombie host
Tấn công “many-to-one”
+Tấn công Man in the Middle (MITM)
Là một loại tấn công mạng mà hacker sẽ đứng giữa người dùng và ứng dụng. Kẻ tấn công chặn và kiểm soát toàn bộ quá trình giao tiếp giữa hai bên để người dùng tin rằng họ vẫn đang trực tiếp liên lạc với nhau.

Những kẻ tấn công sẽ nắm bắt hết mọi thông tin trao đổi kể cả những thông tin nhạy cảm như số tài khoản, số thẻ tín dụng…để đánh cắp danh tính, chuyển tiền hay gây ra các vụ lừa đảo.

1. Tấn công XSS (Cross-Site Scripting):

Cách thức tấn công:

Cross-Site Scripting là lỗ hổng bảo mật cho phép những kẻ tấn công đưa mã độc vào một trang web hợp pháp.
Các tập lệnh này có được quyền của các tập lệnh được tạo bởi trang web mục tiêu và do đó có thể ảnh hưởng đến tính bảo mật và tính toàn vẹn của việc truyền dữ liệu giữa trang web và khách hàng.
Các trang web dễ bị tấn công nếu chúng hiển thị dữ liệu do người dùng cung cấp từ các request hoặc form mà không làm sạch dữ liệu trước khi thực thi

- Kẻ tấn công chèn mã JavaScript độc hại vào trang web không được bảo mật.
- Mã độc hại này có thể được sử dụng để đánh cắp thông tin cá nhân của người dùng, như cookie, mật khẩu, thông tin thẻ tín dụng.
- Mã độc hại cũng có thể được sử dụng để điều khiển trình duyệt của người dùng và thực hiện các hành động trái phép, như tải xuống phần mềm độc hại hoặc chuyển hướng người dùng đến các trang web độc hại.

Cách phòng thủ:

- **Đối với chủ sở hữu trang web:**
    - Sử dụng các biện pháp bảo mật để ngăn chặn kẻ tấn công chèn mã độc hại vào trang web, như:
        - Xác thực đầu vào của người dùng một cách cẩn thận.
        - Sử dụng HTTP Content Security Policy (CSP) để hạn chế các mã JavaScript có thể được thực thi trên trang web.
        - Cập nhật phần mềm và ứng dụng web thường xuyên để vá các lỗ hổng bảo mật.
- **Đối với người dùng:**
    - Cẩn thận với các trang web không đáng tin cậy.
    - Sử dụng trình duyệt có hỗ trợ bảo mật XSS.
    - Cài đặt phần mềm chống virus và phần mềm chống lừa đảo.

2. Tấn công DDoS (Distributed Denial-of-Service):

Cách thức tấn công:

- Kẻ tấn công sử dụng một mạng lưới botnet để gửi nhiều yêu cầu truy cập đến một hệ thống mạng hoặc dịch vụ web cùng lúc.
- Mục đích là làm quá tải hệ thống mạng hoặc dịch vụ web, khiến nó không thể đáp ứng các yêu cầu hợp pháp của người dùng.

Cách phòng thủ:

- **Đối với chủ sở hữu hệ thống mạng hoặc dịch vụ web:**
  - Sử dụng dịch vụ chống DDoS.
  - Cấu hình tường lửa để chặn các yêu cầu truy cập độc hại.
  - Giám sát lưu lượng truy cập mạng để phát hiện các hoạt động bất thường.
- **Đối với người dùng:**
  - Sử dụng các dịch vụ Internet đáng tin cậy.
  - Cập nhật phần mềm và hệ điều hành thường xuyên để vá các lỗ hổng bảo mật.

3. Tấn công Phishing:

Cách thức tấn công:

- Kẻ tấn công gửi email giả mạo từ một tổ chức đáng tin cậy, như ngân hàng hoặc công ty thẻ tín dụng, cho người dùng.
- Email giả mạo yêu cầu người dùng nhấp vào một liên kết đến một trang web giả mạo trông giống như trang web thật của tổ chức.
- Khi người dùng nhập thông tin cá nhân của mình vào trang web giả mạo, kẻ tấn công sẽ đánh cắp thông tin đó.

Cách phòng thủ:

- **Đối với người dùng:**
  - Cẩn thận với các email và trang web không mong muốn.
  - Kiểm tra kỹ địa chỉ trang web trước khi nhập thông tin cá nhân.
  - Không bao giờ nhấp vào các liên kết hoặc tệp đính kèm trong email từ những người bạn không quen biết.
  - Sử dụng phần mềm chống virus và phần mềm chống lừa đảo.

4. Tấn công Man-in-the-middle:

Cách thức tấn công:

Giả mạo IP
Giả mạo hệ thống tên miền (giả mạo DNS)
Giả mạo HTTPS
Đánh cắp lớp cổng bảo mật (SSL)
Đánh cắp email
Nghe trộm wifi
Đánh cắp session

Nhiễm độc bộ nhớ cache

- Kẻ tấn công chặn lưu lượng truy cập mạng giữa hai thiết bị và thay đổi hoặc giám sát lưu lượng truy cập đó.

- Kẻ tấn công có thể sử dụng các kỹ thuật như:
    - Thiết lập mạng Wi-Fi giả mạo.
    - Sử dụng phần mềm độc hại để chặn lưu lượng truy cập mạng.
    - Giải mã lưu lượng truy cập mạng được mã hóa.

Cách phòng thủ:

- **Đối với người dùng:**
    - Sử dụng VPN khi truy cập mạng Wi-Fi công cộng.
    - Cài đặt phần mềm chống virus và phần mềm chống phần mềm độc hại.
    - Sử dụng HTTPS thay vì HTTP khi truy cập các trang web.
    - Cẩn thận với các mạng Wi-Fi công cộng không được bảo mật.

5. Tấn công Injection:

Cách thức tấn công:

Khai thác lỗ hổng bảo mật SQL injection
Có thể thực hiện khi website có lỗ hổng bảo mật có thể gây ra SQL injection
Kẻ tấn công có thể gửi một yêu cầu với các tham số để thực hiện cuộc tấn công SQL injection => cho phép xâm nhập cơ sở dữ liệu, thông tin đăng nhập của người dùng và trong một số cấu hình nhất định, truy cập vào hệ điều hành

- Kẻ tấn công chèn mã độc hại vào truy vấn SQL hoặc mã JavaScript để thực thi các hành động trái phép, như:
    - Truy cập vào cơ sở dữ liệu.
    - Chèn mã độc hại vào trang web.
    - Thực hiện các hành động trái phép trên hệ thống.

Cách phòng thủ:

Đối với chủ sở hữu hệ thống mạng hoặc ứng dụng web:

- Sử dụng các tham số được chuẩn bị
- Cập nhật phần mềm và ứng dụng web thường xuyên
- Sử dụng tường lửa ứng dụng web (WAF)
- Thực hiện kiểm tra bảo mật thường xuyên
- Nâng cao nhận thức về bảo mật cho nhân viên

Đối với người dùng:

- Cẩn thận với các trang web không đáng tin cậy
- Không nhập thông tin cá nhân vào các trang web không an toàn
- Cập nhật trình duyệt và phần mềm chống virus thường xuyên
- Sử dụng mật khẩu mạnh và duy trì chúng một cách an toàn:
- Cẩn thận với các email và tin nhắn không mong muốn

+Social Engineering

- Social engineering sử dụng sự ảnh hưởng và sự thuyết phục để đánh
- lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó

Kẻ tấn công có thể lợi dụng các đặc điểm sau của con người để tấn công:
Mong muốn trở nên hữu dụng
Tin người
Nỗi sợ gặp rắc rối
Đơn giản đến mức cẩu thả

Nhân viên gián điệp/giả mạo
Giả làm người cần được giúp đỡ
Giả làm người quan trọng
Giả làm người được ủy quyền
Giả làm nhân viên hỗ trợ kỹ thuật

Bảo vệ/Ngăn chặn
Hỗ trợ khả năng hạn chế hoặc ngăn chặn tác động của mối đe dọa an ninh mạng.
Bao gồm:
◦ Kiểm soát truy cập;
◦ Nhận thức và đào tạo;
◦Bảo mật dữ liệu;
◦ Quy trình, thủ tục bảo vệ thông tin;
◦Bảo trì
◦Công nghệ/dịch vụ bảo mật

Phát hiện
Cho phép phát hiện kịp thời các sự cố an ninh mạng
Bao gồm:
◦ Phát hiện các thao tác bất thường
◦ Giám sát liên tục an ninh
◦ Quy trình phát hiện

Ứng phó
Thực hiện hành động thích hợp với sự cố an ninh mạng được phát hiện nhằm hỗ trợ khả năng ngăn chặn tác động của sự cố an ninh mạng, giảm thiểu thiệt hại
Bao gồm:
◦ Lập kế hoạch ứng phó
◦ Truyền thông
◦ Phân tích

◦ Giảm thiểu thiệt hại
◦Cải tiến

Phục hồi
Các hoạt động thích hợp để khôi phục hoạt động kinh doanh hoặc dịch vụ nào bị thiệt hại do sự cố an ninh mạng, hỗ trợ phục hồi kịp thời các hoạt động bình thường để giảm tác động từ sự cố an ninh mạng.
Bao gồm:
◦ Lập kế hoạch phục hồi
◦Cải tiến
◦ Truyền thông

5) Ôn tập kiến thức về IP broadcast, IP unicast, MAC broadcast, cơ chế chuyển mạch logic và chuyển mạch IP.

1. IP Broadcast và IP Unicast:

- **IP Broadcast:**
  - Là phương thức truyền dữ liệu đến tất cả các thiết bị trên cùng một mạng con.
  - Địa chỉ IP broadcast mặc định là 255.255.255.255.
  - Sử dụng cho các mục đích như:
    - Tìm kiếm máy chủ DHCP.
    - Gửi thông báo mạng.
    - Truyền tin cho tất cả các thiết bị trên mạng.
- **IP Unicast:**
  - Là phương thức truyền dữ liệu đến một thiết bị cụ thể trên mạng.
  - Sử dụng địa chỉ IP của thiết bị đích để truyền dữ liệu.
  - Là phương thức truyền dữ liệu phổ biến nhất trên mạng IP.

2. MAC Broadcast:

- Là phương thức truyền khung dữ liệu đến tất cả các thiết bị trên cùng một đoạn mạng LAN.
- Địa chỉ MAC broadcast mặc định là FF:FF:FF:FF:FF:FF.
- Sử dụng cho các mục đích như:
  - Tìm kiếm địa chỉ MAC của thiết bị đích.
  - Gửi thông báo mạng cục bộ.
  - Truyền tin cho tất cả các thiết bị trên cùng một đoạn mạng LAN.

3. Cơ chế chuyển mạch logic:

- Là cơ chế chuyển mạch dựa trên địa chỉ MAC của thiết bị đích.
- Khi một thiết bị gửi khung dữ liệu, bộ chuyển mạch sẽ đọc địa chỉ MAC đích trong khung dữ liệu và chuyển khung dữ liệu đến cổng kết nối với thiết bị đích.

- Cơ chế chuyển mạch logic giúp cải thiện hiệu suất mạng bằng cách giảm thiểu lưu lượng truy cập broadcast và unicast không cần thiết.

4. Chuyển mạch IP:

- Là cơ chế chuyển mạch dựa trên địa chỉ IP của thiết bị đích.
- Khi một thiết bị gửi gói tin IP, bộ chuyển mạch IP sẽ đọc địa chỉ IP đích trong gói tin và chuyển gói tin đến cổng kết nối với thiết bị đích.
- Chuyển mạch IP giúp cải thiện hiệu suất mạng bằng cách giảm thiểu lưu lượng truy cập broadcast và unicast không cần thiết, đồng thời cũng cung cấp các tính năng bảo mật nâng cao như danh sách kiểm soát truy cập (ACL).

6) Các kỹ thuật tấn công Layer 2: tấn công ARP, tấn công DHCP, tấn công DNS: mục đích cách thức?

1. Tấn công ARP (Address Resolution Protocol):

Mục đích:

- Lấy cắp thông tin nhạy cảm bằng cách nghe lén lưu lượng truy cập mạng.
- Chặn hoặc sửa đổi lưu lượng truy cập mạng.
- Giả mạo máy chủ hợp pháp để đánh lừa người dùng.

Cách thức:

- Kẻ tấn công gửi các gói tin ARP giả mạo đến các thiết bị trên mạng để liên kết địa chỉ IP với địa chỉ MAC sai.
- Khi một thiết bị trên mạng muốn gửi gói tin đến một thiết bị khác, nó sẽ gửi yêu cầu ARP để tìm địa chỉ MAC của thiết bị đích.
- Kẻ tấn công có thể chặn yêu cầu ARP này và gửi phản hồi ARP giả mạo, cho biết địa chỉ MAC của kẻ tấn công được liên kết với địa chỉ IP của thiết bị đích.
- Khi thiết bị trên mạng gửi gói tin đến thiết bị đích, nó sẽ gửi gói tin đến địa chỉ MAC của kẻ tấn công thay vì địa chỉ MAC thực sự của thiết bị đích.
- Kẻ tấn công có thể nghe lén hoặc sửa đổi lưu lượng truy cập mạng được gửi đến địa chỉ MAC của mình.

2. Tấn công DHCP (Dynamic Host Configuration Protocol):

Mục đích:

- Kiểm soát lưu lượng truy cập mạng bằng cách giả mạo máy chủ DHCP hợp pháp.
- Hướng người dùng đến các trang web độc hại.
- Thu thập thông tin cá nhân của người dùng.

Cách thức:

- Kẻ tấn công cài đặt máy chủ DHCP giả mạo trên mạng.

- Khi một thiết bị trên mạng kết nối với mạng, nó sẽ gửi yêu cầu DHCP để xin cấp địa chỉ IP, máy chủ DHCP giả mạo sẽ cấp cho thiết bị địa chỉ IP và các thông tin cấu hình mạng khác.
- Khi người dùng truy cập internet, họ sẽ được chuyển hướng đến các trang web độc hại do kẻ tấn công kiểm soát.
- Kẻ tấn công có thể thu thập thông tin cá nhân của người dùng từ các trang web độc hại này.

3. Tấn công DNS (Domain Name System):

Mục đích:

- Hướng người dùng đến các trang web độc hại.
- Thu thập thông tin cá nhân của người dùng.
- Ngăn người dùng truy cập các trang web hợp pháp.

Cách thức:

- Kẻ tấn công tấn công máy chủ DNS và sửa đổi các bản ghi DNS để liên kết các tên miền hợp pháp với địa chỉ IP của các trang web độc hại.
- Khi người dùng truy cập một trang web hợp pháp, họ sẽ được chuyển hướng đến trang web độc hại do kẻ tấn công kiểm soát.
- Kẻ tấn công có thể thu thập thông tin cá nhân của người dùng từ các trang web độc hại này.
- Kẻ tấn công có thể sửa đổi các bản ghi DNS để ngăn người dùng truy cập các trang web hợp pháp.

THAM KHẢO&HƯỚNG DẪN LO1&2

Hiểm họa, rủi ro, tấn công và lỗ hổng

Hiểm họa, rủi ro, tấn công và lỗ hổng là những khái niệm cốt lõi của an toàn thông tin. Tuy nhiên, các thuật ngữ này thường xuyên bị sử dụng nhầm lẫn và chồng chéo lẫn nhau. Mặc dù có những mối liên hệ nhất định giữa các khái niệm này, nhưng chúng là các thuật ngữ riêng biệt với ý nghĩa khác nhau. Bài viết này sẽ trình bày và phân biệt sự khác nhau giữa các khái niệm này.

Hiểm họa

Hiểm họa an toàn thông tin là những khả năng tác động lên thông tin hoặc hệ thống thông tin dẫn tới sự thay đổi, hư hại, sao chép, sự ngăn chặn tiếp cận tới thông tin; phá huỷ hoặc làm ngừng trệ hoạt động của vật mang thông tin. Hiểm họa an toàn thông tin đề cập đến các tình huống hoặc sự kiện có khả năng tác động gây hại đến hệ thống thông tin.

Hiểm họa có thể chia thành 3 loại phổ biến: các hiểm họa tự nhiên (bão hoặc lũ lụt), các hiểm họa không chủ ý (chẳng hạn như một nhân viên truy cập sai thông tin, quản trị viên vô tình để dữ liệu không được bảo vệ trên hệ thống gây lộ lọt, rò rỉ dữ liệu) và các hiểm họa có chủ ý.

Có rất nhiều các hiểm họa có chủ ý như các cuộc tấn công mạng, mã độc, phần mềm gián điệp, phần mềm quảng cáo, lừa đảo hoặc kỹ nghệ xã hội dẫn đến việc kẻ tấn công cài đặt trojan và đánh cắp thông tin cá nhân từ các ứng dụng của bạn hoặc hành động của một nhân viên bất mãn nhằm đánh cắp có chủ đích các dữ liệu quan trọng trong tổ chức.

Gần đây nhất, vào ngày 12 tháng 5 năm 2017, Ransomware WannaCry đã bắt đầu tấn công các máy tính và mạng trên toàn cầu và từ đó được mô tả là cuộc tấn công lớn nhất của loại hình tội phạm này. Tội phạm mạng liên tục đưa ra những cách sáng tạo mới để tấn công và thỏa hiệp dữ liệu của bạn.

Trong an toàn thông tin các hiểm họa có xu hướng được cụ thể hóa đối với từng môi trường nhất định. Ví dụ một số loại mã độc có thể rất nguy hiểm trên hệ điều hành Windows, tuy nhiên lại không có bất kỳ tác dụng gì trên hệ điều hành Linux...

Các hiểm họa an ninh mạng được thực hiện bởi các tác nhân đe dọa. Các tác nhân đe dọa thường là những người hoặc thực thể có khả năng khởi đầu một hiểm họa tiềm ẩn đối với hệ thống. Ví dụ tội phạm có động cơ tài chính (tội phạm mạng), động cơ chính trị (kẻ tấn công), đối thủ cạnh tranh, nhân viên bất cẩn, nhân viên bất mãn và những kẻ tấn công được hậu thuẫn bởi các tổ chức chính phủ, quốc gia khác. Mặc dù các thảm họa tự nhiên, cũng như các sự kiện chính trị và môi trường khác cũng tạo thành các mối hiểm họa an toàn thông tin, nhưng chúng thường không được coi là tác nhân đe dọa (điều này không có nghĩa là các hiểm họa đó có thể được coi nhẹ hoặc ít quan trọng hơn).

Các hiểm họa an toàn thông tin cũng có thể trở nên nguy hiểm hơn nếu các tác nhân đe dọa tận dụng một hoặc nhiều lỗ hổng để có quyền truy cập vào hệ thống, thường bao gồm cả hệ điều hành.

Lổ hổng

Lỗ hổng đề cập đến các điểm yếu mà có thể được sử dụng để gây hại cho một hệ thống, là những khiếm khuyết trong chức năng, thành phần nào đó của hệ thống thông tin mà có thể bị lợi dụng để gây hại cho hệ thống. Về mặt bản chất, lỗ hổng là những điểm yếu có thể bị khai thác bởi các hiểm họa nhằm gây hại cho hệ thống. Nói cách khác, đây là một vấn đề đã biết cho phép một cuộc tấn công diễn ra thành công. Ví dụ: khi một nhân viên trong công ty từ chức và bạn quên vô hiệu hóa quyền truy cập của họ vào tài khoản từ bên ngoài có thể tạo ra những lỗ hổng an toàn cho các hiểm họa có chủ ý hoặc vô ý.

Một hệ thống có thể được khai thác thông qua một lỗ hổng duy nhất, ví dụ, một cuộc tấn công SQL Injection duy nhất có thể cung cấp cho kẻ tấn công toàn quyền kiểm soát dữ liệu nhạy cảm. Kẻ tấn công cũng có thể xâu chuỗi và tạo ra một chuỗi các tấn công sử dụng một số cách khai thác với nhau, lợi dụng nhiều hơn một lỗ hổng để giành quyền kiểm soát nhiều hơn đối với hệ thống.

Lỗ hổng có thể xuất hiện ở khắp mọi nơi, đó có thể là một lỗ hổng của hệ điều hành, một ứng dụng, thậm chí ở một vị trí vật lý trong văn phòng, một trung tâm dữ liệu được phân bố hoạt động vượt quá khả năng cho phép của hệ thống làm mát, thiếu máy phát điện dự phòng hoặc các yếu tố khác.

Mộ số lỗ hổng phổ biến mà chúng ta hay gặp trên thực tế là SQL Injection, XSS, cấu hình sai máy chủ, truyền dữ liệu nhạy cảm dưới dạng bản rõ,...

Hiểu rõ về các lỗ hổng là bước đầu tiên để quản lý rủi ro cho hệ thống thông tin. Các hiểm họa khai thác các lỗ hổng để tạo nên các rủi ro đối với hệ thống.

Rủi ro

Rủi ro là khả năng một cái gì đó xấu sẽ xảy ra ví dụ như: các tổn thất tài chính do sự gián đoạn kinh doanh, mất quyền riêng tư, thiệt hại về mặt danh tiếng, liên đới đến các vấn đề pháp lý và thậm chí có thể bao gồm mất mạng. Rủi ro đề cập đến khả năng mất mát hoặc thiệt hại khi các hiểm họa khai thác lỗ hổng. Để một rủi ro xảy ra trong một môi trường cụ thể thì cần phải có cả một hiểm họa và một lỗ hổng mà hiểm họa cụ thể có thể khai thác. Ví dụ nếu chúng ta có một hệ thống máy tính, chúng ta có hiểm họa (mất điện) và một điểm yếu (lỗ hổng) phù hợp với nó (không có bộ lưu điện). Trong trường hợp này chúng ta chắc chắn có một rủi ro (tắt máy). Tuy nhiên, ngược lại, nếu chúng ta vẫn có cùng hiểm họa là mất điện, nhưng hệ thống máy tính lúc này lại có bộ lưu điện, chúng ta sẽ không còn rủi ro tắt máy trong trường hợp này bởi vì hiểm họa của chúng ta ở đây không có lỗ hổng để khai thác.

Rủi ro có thể được định nghĩa như sau:

Rủi ro = Hiểm họa x Lỗ hổng

Bạn có thể giảm nguy cơ rủi ro bằng cách tạo và thực hiện kế hoạch quản lý rủi ro. Và để quản lý rủi ro hiệu quả, bạn cần đánh giá mức độ rủi ro:

Mức độ rủi ro = Xác suất xảy ra rủi ro * Thiệt hại ước tính

Ví dụ:

Chúng ta có SQL Injection là một lỗ hổng

Hiểm họa trộm dữ liệu nhạy cảm là một trong những mối đe dọa lớn nhất có thể xảy ra với lỗ hổng SQL Injection.

Những kẻ tấn công có động cơ tài chính là một trong những tác nhân đe dọa.

Rủi ro xảy ra khi dữ liệu nhạy cảm bị đánh cắp đó là các chi phí tài chính đáng kể (tổn thất tài chính và danh tiếng) cho doanh nghiệp

Xác suất của một cuộc tấn công như vậy là rất cao, do SQL Injection là một lỗ hổng dễ tiếp cận, được khai thác rộng rãi và dễ dàng do các trang web thường phải tương tác với bên ngoài. Do đó, lỗ hổng SQL Injection trong kịch bản này phải được coi là lỗ hổng có mức độ rủi ro cao.

Kết luận

Để tóm tắt lại các khái niệm về hiểm họa, lỗ hổng và rủi ro, chúng ta sử dụng ví dụ về một cơn bão trong thế giới thực.

Hiểm họa từ một cơn bão nằm ngoài tầm kiểm soát của chúng ta. Tuy nhiên, chúng ta biết rằng một cơn bão có thể có khả năng gây thiệt hại cho hệ thống và lúc này chúng ta cần đánh giá khả năng và mức độ thiệt hại có thể có đồng thời đánh giá các điểm yếu có thể xuất hiện đối với cơn bão và đưa ra một kế hoạch hành động để giảm thiểu tác động từ bão. Trong trường hợp này, một lỗ hổng của hệ thống sẽ là không có kế hoạch khôi phục dữ liệu trong

trường hợp thiết bị lưu trữ vật lý của bạn bị hư hại do gió bão lốc hoặc mưa lớn. Rủi ro đối với doanh nghiệp của bạn sẽ là mất thông tin hoặc gián đoạn trong kinh doanh do không giải quyết được các lỗ hổng của bạn.

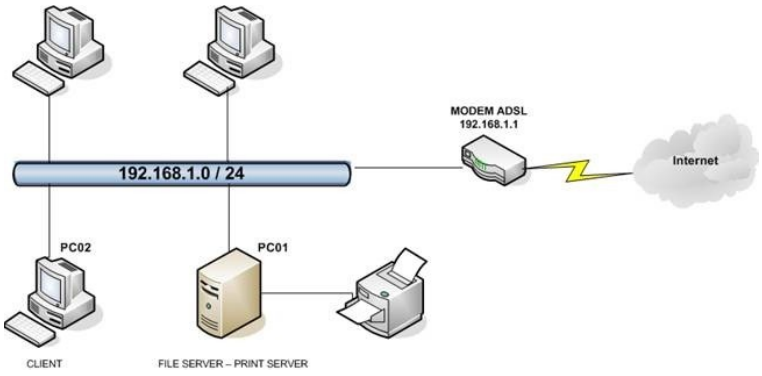
Việc hiểu chính xác các định nghĩa của các thành phần bảo mật này sẽ giúp bạn hiệu quả hơn trong việc thiết kế một khung để xác định các mối đe dọa tiềm ẩn, phát hiện và giải quyết các lỗ hổng của bạn để giảm thiểu rủi ro.

Sự khác biệt giữa lỗ hổng và hiểm họa, giữa lỗ hổng và rủi ro thường khá dễ hiểu. Tuy nhiên, sự khác biệt giữa hiểm họa và rủi ro có thể mang nhiều sắc thái hơn. Việc hiểu được sự khác biệt về thuật ngữ này cho phép khả năng liên kết rõ ràng hơn giữa các nhóm bảo mật và các bên khác nhau nhằm giúp hiểu rõ hơn về các mối đe dọa tiềm ẩn và ảnh hưởng của nó khi gây ra các rủi ro đến hệ thống. Sự hiểu biết tốt cũng là điều cần thiết để đánh giá rủi ro và quản lý rủi ro hiệu quả, đồng thời giúp thiết kế các giải pháp bảo mật, cũng như để xây dựng một chính sách bảo mật và chiến lược an ninh mạng tối ưu phù hợp cho tổ chức.

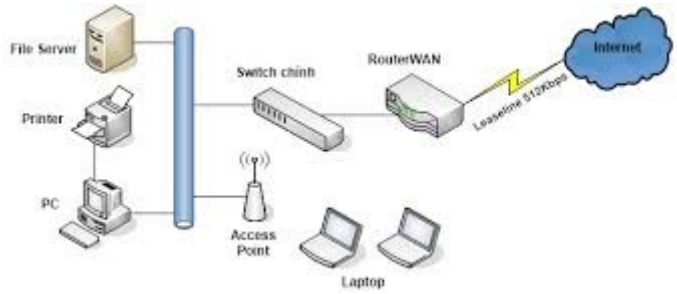
Ví dụ:

Các sơ đồ sau đây được cho là không bảo đảm an toàn, tiềm ẩn nhiều mối hiểm hoạ đe doạ an ninh hệ thống:

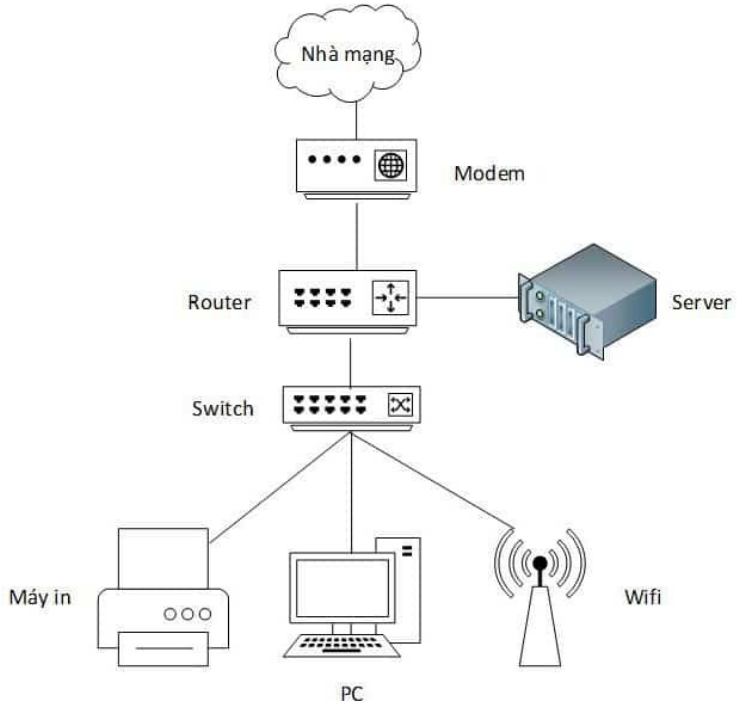
Sơ đồ 1:



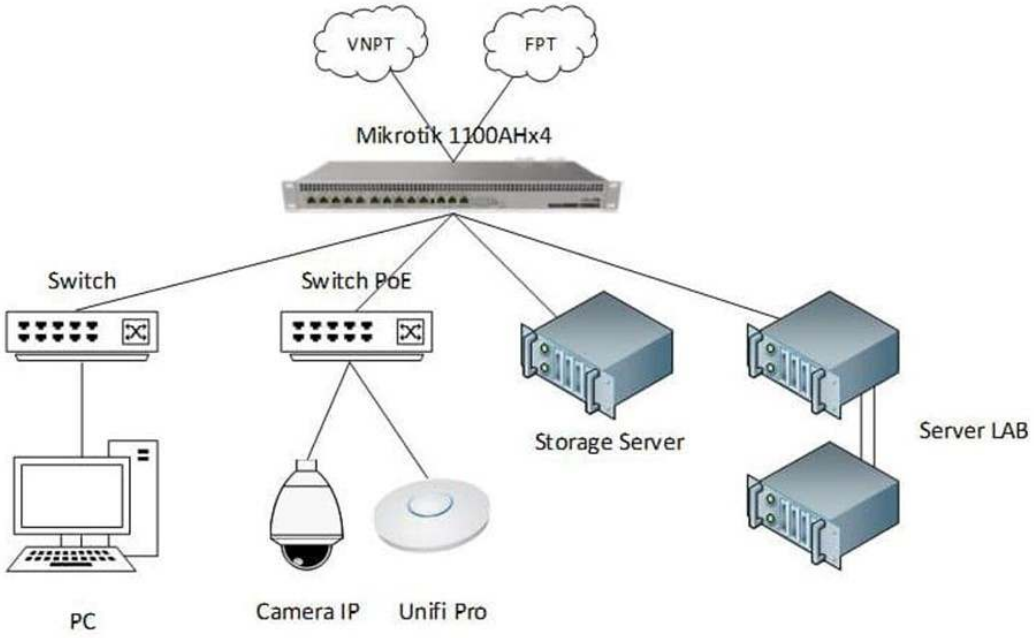
Sơ đồ 2:



Sơ đồ 3:



Sơ đồ 4:



Các sơ đồ trên sẽ tiềm ẩn các mối hiểm hoạ như:

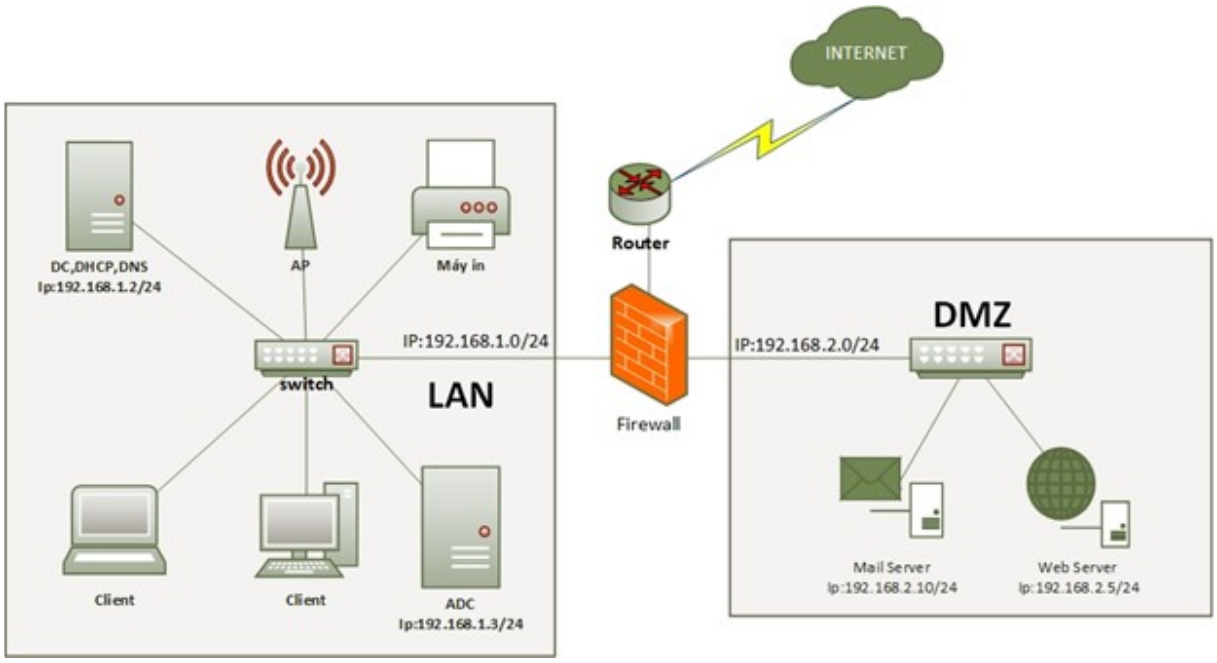
1- Hệ thống chưa cho thấy có giải pháp khi mất dữ liệu xảy ra
2- Do không có tường lửa kiểm soát truy cập tập trung nên người dùng bên trong hệ thống dễ bị nhiễm ransomware
3- Sơ đồ 1, 2, 3: Nếu đường mạng interet bị mất kết nối thì toàn bộ hệ thống bị gián đoạn kết nối internet.
4- Do không có lớp tường lửa bảo vệ giám sát nên các máy tính bên trong dễ dàng truy cập tới các địa chỉ không tin cậy bên ngoài và dễ bị ăn cắp thông tin
5- Server không được bảo vệ bởi Firewall nên hacker bên ngoài có thể tấn công trực diện
6- Kẻ tấn công có thể sử dụng các công cụ hack wifi và thực hiện tấn công ARP rồi sử dụng Packet Sniffing để ăn cắp thông tin.
7- ….

Giải pháp:

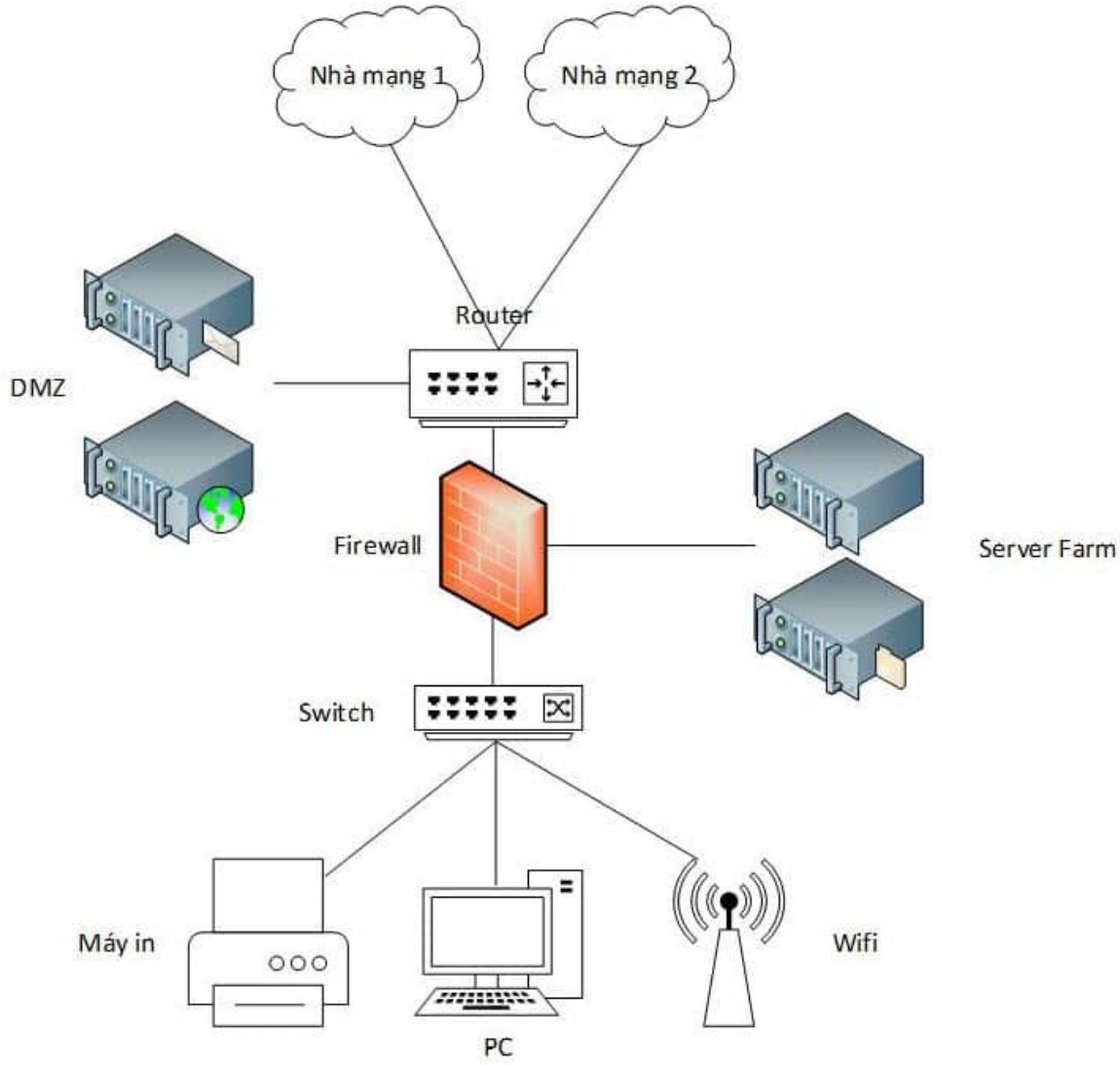
1- Tăng cường an ninh cho hệ thống với thiết lập các chính sách Policies cho mật khẩu
2- Thiết lập tường lửa để bảo vệ, thiết lập vùng DMZ đưa Server vào vùng DMZ.
3- Tăng cường bảo mật email với ứng dụng Digital signature
4- Thiết lập hệ thống giám sát mạng bằng Zabbix server
5- Xây dựng Domain Controller để quản trị xác thực người dùng tập trung
6- Sử dụng Wifi Controller để tăng cường kiểm soát Wifi
7- Thêm đường kết nối internet để gia tăng tính sẵn sàng High Availability (HA)
8- ….

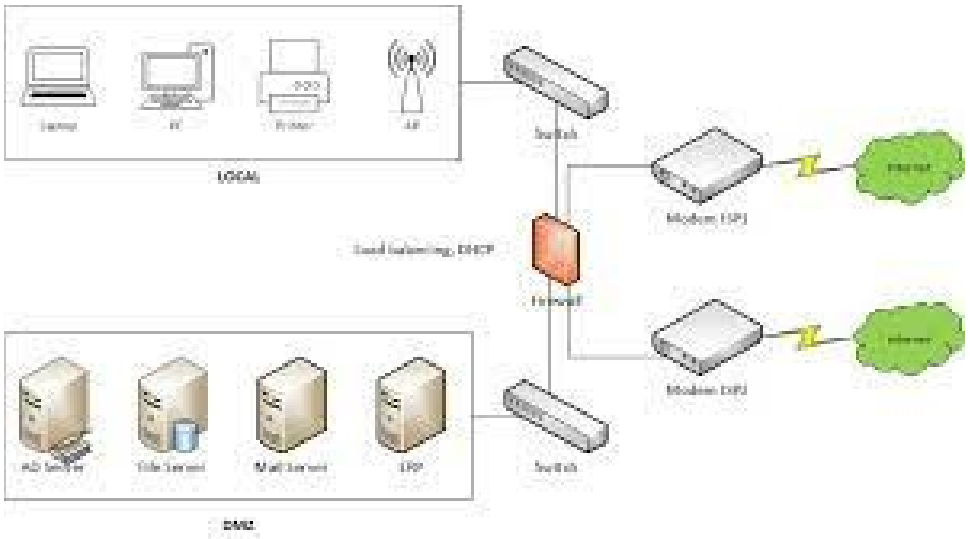
Các sơ đồ sau là có triển khai các giải pháp tăng cường an ninh hệ thống cho các sơ đồ trên:

Sơ đồ 1:



Sơ đồ 2:





Sinh viên giải thích được tường lửa kiểm soát truy cập giữa các thành phần sơ đồ mạng:

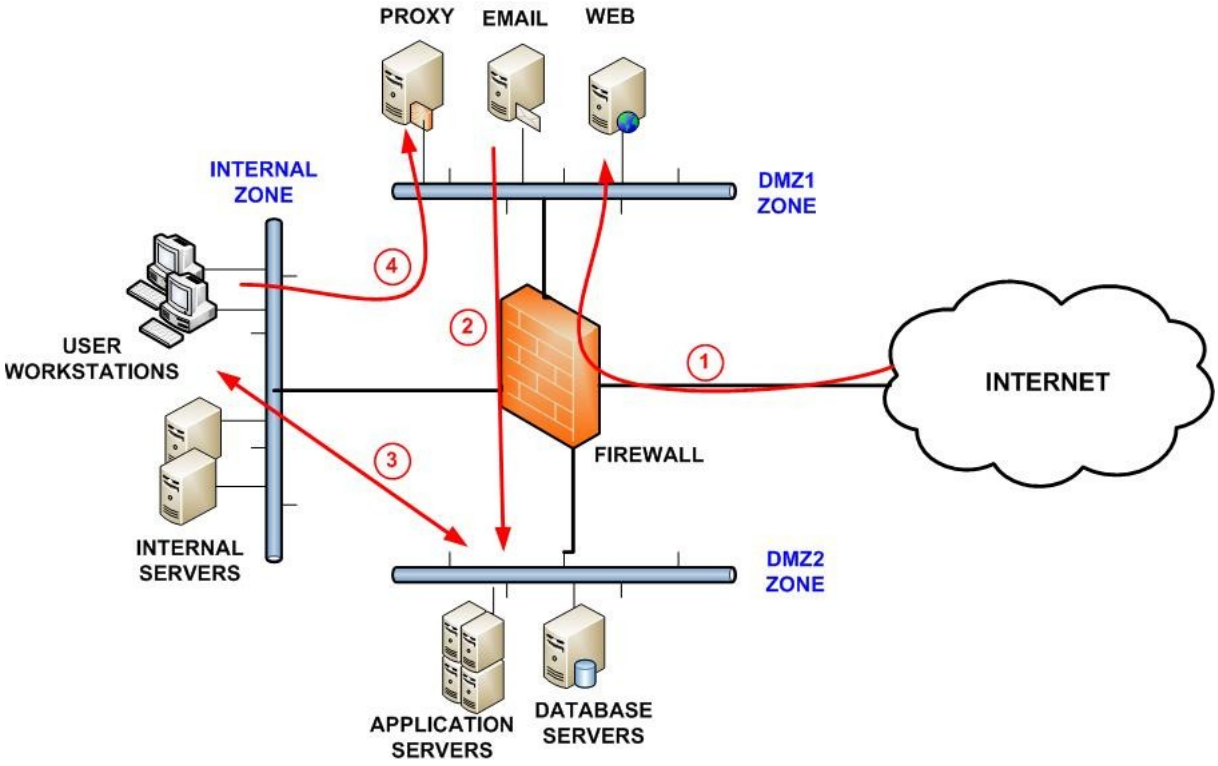
Tường lửa kiểm soát truy cập (firewall) là một thành phần quan trọng trong bất kỳ hệ thống mạng nào, đặc biệt là trong việc bảo vệ chống lại các cuộc tấn công và xâm nhập từ bên ngoài. Đối với một kỹ sư chuyên về an ninh hệ thống, việc hiểu và triển khai tường lửa một cách hiệu quả là rất quan trọng.

Tường lửa kiểm soát truy cập hoạt động bằng cách quản lý và kiểm soát lưu lượng thông tin đi vào và ra khỏi mạng. Cụ thể, tường lửa có thể thiết lập các quy tắc để xác định liệu một gói tin dữ liệu nào có được phép đi qua hay không dựa trên các điều kiện như địa chỉ IP nguồn và đích, cổng giao tiếp, loại giao thức, và nhiều yếu tố khác.

Trong sơ đồ mạng, tường lửa thường được đặt ở các điểm chiến lược như biên giới của mạng nội bộ và mạng internet, hoặc giữa các phân đoạn mạng khác nhau bên trong mạng nội bộ. Tại mỗi điểm này, tường lửa có thể cấu hình để kiểm soát truy cập giữa các thành phần của mạng theo các quy tắc được xác định trước.

Ví dụ, tường lửa có thể được cấu hình để chặn tất cả các yêu cầu truy cập đến từ một phân đoạn mạng nội bộ đến một máy chủ ngoài cùng trên internet nếu không được phép. Nó cũng có thể kiểm tra và chặn các gói tin độc hại hoặc không mong muốn từ internet trước khi chúng đến được máy chủ trong mạng nội bộ.

Tóm lại, tường lửa kiểm soát truy cập giữa các thành phần sơ đồ mạng bằng cách thiết lập và thực thi các quy tắc an ninh, giúp bảo vệ hệ thống khỏi các mối đe dọa từ bên ngoài và kiểm soát lưu lượng thông tin trong mạng nội bộ một cách hiệu quả.



THAM KHẢO&HƯỚNG DẪN cho LO3 – Bài thu hoạch kiến thức về ACM

Sinh viên cần đọc rõ tình huống cụ thể và tra cứu vào bộ quy tắc ứng xử để xem xét phân tích cá nhân hành động trong tình huống đó vi phạm vào điều lệ nào trong bộ quy tắc ứng xử cũng như vi phạm điều luật an ninh mạng và hình thức xử lý.

Một số tình huống mẫu để sinh viên phân tích:

Người quản trị hệ thống website của 1 ngân hàng phát hiện ra cơ chế thực hiện backup và Restore của hệ thống có vấn đề và nó đã không hoạt động hơn 6 tháng nay. Tuy nhiên anh ta

không biết cách khắc phục và anh ta cũng không báo cho ban giám đốc. Tháng vừa rồi hệ thống Website bị sự cố và cần các bản backup để restore hệ thống thì không có để thực hiện.

- *Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử của người quản trị.*
- *Nếu ở vị trí người quản trị hệ thống, bạn sẽ hành xử như thế nào?*

Một nhân viên IT của công ty đầu tư chứng khoán có thể theo dõi và đọc được emails, documentations, thậm chí ghi băng được những trao đổi CEO, CFO và điều này sẽ giúp nhân viên đó mua bán stocks hữu hiệu, kiếm được nhiều tiền cho bản thân hoặc bán tin tức cho những đối thủ cạnh tranh... Trong một lần uống café nhân viên IT đó đã tiết lộ thông tin bảo mật cho một người bạn thân và sau đó nhận về một số tiền gọi là quà là 100 ngàn đô.

1. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của bạn A.
2. Nếu ở vị trí người người A, bạn sẽ hành xử như thế nào?

Bạn làm cho công ty chuyên thiết kế Website cho các khách hàng. Ban lãnh đạo của công ty luôn yêu cầu bạn dùng chính Website của khách hàng mà công ty thiết kế để đặt backlinks đến Website công ty mình. Mục tiêu là SEO Website cho công ty. Các khách hàng không hề biết việc làm này của công ty. Và điều đáng nói hơn nữa là có những website công ty đặt backlink thông qua một dòng text có fontsize nhỏ (2px), màu chữ trắng vì sợ khách hàng biết và phàn nàn. Bạn đã làm đều này từ nhiều năm trước đến nay.

- *Dựa vào qui tắc ứng xử ACM (Association for Computing Machinery), Anh/Chị hãy cho biết Ban lãnh đạo của công ty vi phạm nguyên tắc nào? Giải thích ý nghĩa của nguyên tắc đó và tính đúng/sai của Ban lãnh đạo công ty trên.*
- *Dựa vào Luật An ninh mạng Việt Nam (Luật số: 24/2018/QH14), Anh/Chị hãy cho biết Ban lãnh đạo của công ty vi phạm điều luật nào? Giải thích ý nghĩa của điều luật đó và tính đúng/sai của hành vi trên.*

Bạn là kỹ sư phần mềm tại một công ty mới thành lập. Công ty đang phát triển một ứng dụng mới cho phép nhân viên bán hàng tạo ra và gửi email báo giá bán hàng và hóa đơn của khách hàng từ điện thoại thông minh của họ. Bộ phận maketing của công ty bạn đã giới thiệu ứng dụng này cho một tập đoàn lớn và nói rằng ứng dụng này hiện nay đã sẵn sàng. Nhưng thực tế, tại thời điểm này ứng dụng vẫn còn chứa khá nhiều lỗi, cần phải hơn 1 tháng thì ứng dụng mới được khắc phục các lỗi nghiêm trọng. Tuy nhiên, trưởng nhóm testing đã báo cáo rằng tất cả các lỗi đã được tìm ra và có thể khắc phục dễ dàng. Do sự cạnh tranh khốc liệt trong ngành công nghiệp phần mềm trên điện thoại thông minh, ban giám đốc quyết định công ty phải là "người đầu tiên" đưa ứng dụng này ra thị trường cho dù vẫn biết ứng dụng chưa hoàn chỉnh. Nếu sản phẩm này không xuất hiện đầu tiên, công ty khởi nghiệp của bạn có thể sẽ bị phá sản. Bạn là người có trách nhiệm đưa sản phẩm đó ra thị trường.

1. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc.

2. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của bạn nếu bạn đồng ý đưa sản phẩm ra trong tuần tới.

3. Nếu bạn muốn đưa sản phẩm ra tuần tới mà không vi phạm quy tắc xứng xử thì bạn sẽ làm gì và giải thích lý do tại sao

Để giám sát tất cả hành động truy cập web của các nhân viên trong công ty. Ban giám đốc đã xây dựng một ứng dụng ghi nhận lại hết tất cả các lịch sử sử dụng máy tính của các nhân viên. Phần mềm ghi nhận lịch sử truy cập web, ghi nhận lại hết thao tác gõ bàn phím, các màn hình máy tính được theo dõi 24/24. Ban giám đốc thường xuyên vào ứng dụng này kiểm soát xem ai đã truy cập nội dung mang tính giải trí trong giờ làm việc hoặc đang làm gì trên màn hình,... nhằm mục tiêu nhắc nhỡ cũng như phạt cảnh cáo các nhân viên vi phạm.

1. Nếu bạn là ban giám đốc - người quyết định giám sát nhân viên bằng hình thức trên thì bạn có thông báo trước cho người dùng hay không?

2. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc này

Một công ty kinh doanh phần mềm sử dụng phần mềm Ptraker. Đây là phần mềm giúp người dùng có thể xem tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh, bật - tắt 3G/GPRS của điện thoại bị giám sát. Thậm chí người sử dụng còn có thể ra lệnh điều khiển từ xa điện thoại bị cài Ptracker bằng cách nhắn tin tới điện thoại này.

1. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người ra quyết định kinh doanh phần mềm này.

2. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người dùng phần mềm trên để theo dõi và điều khiển điện thoại của người khác

Người quản trị mạng của một công ty nhỏ được giao giải quyết mọi vấn đề liên quan đến việc cài đặt, cấu hình các phần cứng cũng như phần mềm trên hệ thống máy tính. Khi cài mới hoặc cập nhật các phần mềm đều có các đề xuất chi tiền mua các phần mềm có bản quyền. Tuy nhiên người quản trị không bao giờ mua các phần mềm có bản quyền đó về cài đặt mà chỉ cài đặt các bản crack. Số tiền mua bản quyền hằng năm người quản trị chiếm đoạt hết. Do dùng các phần mềm crack nên thỉnh thoảng người quản trị phải tìm các key crack trên các trang crack để cấu hình lại các phần mềm.

1. Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người quản trị.

2. Phân tích mối nguy hại của hành vi của người quản trị mạng ảnh hưởng đến doanh nghiệp.

Một số tình huống tìm hiểu Luật An ninh mạng:

Tình huống 1. Do thiếu tiền ăn chơi, A và B đã lập ra nhiều tài khoản facebook ảo để bán điện thoại qua mạng. Hai bạn chụp ảnh những chiếc điện thoại và lấy những hình ảnh trên mạng để đăng bán với giá rẻ hơn so với giá thị trường và đặt ra quy định là khách hàng mua hàng được quyền đổi trả nhưng không được xem hàng trước khi thanh toán tiền. Đến lúc giao hàng, 2 bạn đã bỏ một hộp khẩu trang y tế thay vì điện thoại. Sau đó, 02 bạn xóa tài khoản facebook với mục đích khách hàng sau khi phát hiện sẽ không liên lạc được.

Hỏi, nếu A và B rủ em tham gia thì em có tham gia cùng không? Vì sao?

Gợi ý trả lời:

Không, vì hành vi của A và B là vi phạm pháp luật. Vi phạm điều cấm của **Luật An ninh mạng** (hành vi sử dụng công nghệ thông tin để chiếm đoạt tải sản).

Điều 174 **Bộ luật hình sự 2015** sửa đổi bổ sung quy định về Tội lừa đảo chiếm đoạt tài sản nhưu sau:

Tìm hiểu Luật An ninh mạng 2018

1. Người nào bằng thủ đoạn gian dối chiếm đoạt tài sản của người khác trị giá từ 2.000.000 đồng đến dưới 50.000.000 đồng hoặc dưới 2.000.000 đồng nhưng thuộc một trong các trường hợp sau đây, thì bị phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:

a) Đã bị xử phạt vi phạm hành chính về hành vi chiếm đoạt tài sản mà còn vi phạm;

b) Đã bị kết án về tội này hoặc về một trong các tội quy định tại các điều 168, 169, 170, 171, 172, 173, 175 và 290 của Bộ luật này, chưa được xóa án tích mà còn vi phạm;

c) Gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội;

d) Tài sản là phương tiện kiếm sống chính của người bị hại và gia đình họ96.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 02 năm đến 07 năm:

a) Có tổ chức;

b) Có tính chất chuyên nghiệp;

c) Chiếm đoạt tài sản trị giá từ 50.000.000 đồng đến dưới 200.000.000 đồng;

d) Tái phạm nguy hiểm;

đ) Lợi dụng chức vụ, quyền hạn hoặc lợi dụng danh nghĩa cơ quan, tổ chức;

e) Dùng thủ đoạn xảo quyệt;

g)97 (được bãi bỏ)

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 15 năm:

a) Chiếm đoạt tài sản trị giá từ 200.000.000 đồng đến dưới 500.000.000 đồng;

b)98 (được bãi bỏ)

c) Lợi dụng thiên tai, dịch bệnh.

4. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 12 năm đến 20 năm hoặc tù chung thân:

a) Chiếm đoạt tài sản trị giá 500.000.000 đồng trở lên;

Sự cần thiết ban hành Luật An ninh mạng

b)99 (được bãi bỏ)

c) Lợi dụng hoàn cảnh chiến tranh, tình trạng khẩn cấp.

5. Người phạm tội còn có thể bị phạt tiền từ 10.000.000 đồng đến 100.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

Tình huống 2. A và B là hai bạn rất thân từ khi còn là học sinh tiểu học đến trung học cơ sở, nhưng đến năm lớp 8 thì A và B không còn thân thiết và chơi với nhau nữa.

B đã dùng tài khoản mạng xã hội Facebook để đăng tải các thông tin về bí mật của cá nhân A như tính cách, những đặc điểm trên cơ thể, về gia đình A, nói xấu A…và chia sẻ thông tin này đến bạn bè của A và nhận được nhiều bình luận từ người dùng Facebook. A rất buồn và đã đề nghị B gở bỏ các thông tin nhưng B không gở dẫn đến A phải bỏ học.

Hỏi: Việc B dùng mạng xã hội Facebook để đăng tải các thông tin về bí mật của cá nhân A như tính cách, những đặc điểm trên cơ thể, về gia đình A có đúng pháp luật không? Vì sao

Gợi ý Trả lời:

Hành vi của B là vi phạm pháp luật, vì theo Điều 18 *Luật An ninh mạng* thì Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử Đăng tải, phát tán thông tin trên không gian mạng có nội dung bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân là vi phạm pháp luật.

Hành vi của B sẽ bị xử phạt như thế nào: Phạt tiền từ 10-20 triệu đồng đối với hành vi: Cung cấp, trao đổi, truyền đưa hoặc lưu trữ, sử dụng thông tin số nhằm đe dọa, quấy rối, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của người khác.

Nghị định số 174/2013/NĐ-CP ngày 03/11/2013 của Chính phủ quy định xử phạt vi pham hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện.

Tình huống 3. Theo các bạn khi sử dụng mạng internet, nhất là mạng xã hội như facebook thì chúng ta không được đăng tải, phát tán những nội dung gì?

Gợi ý trả lời:

Theo quy định tại Điều 18 Luật An ninh mạng thì hành vi Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định dưới đây là vi phạm pháp luật:

1. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

2. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm:

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm:

a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

4. Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm:

a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác;

b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

5. Thông tin trên **không gian mạng** có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế – xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

Tình huống 4. Bạn A học lớp 9 rất thích đốt pháo, lân la lên mạng bạn A được một tài khoản facebook mời mua pháo với giá 200k/hộp. A đã nói dối bố mẹ là cần 200k để nộp tiền học, sau khi bố mẹ cho tiền thì A đã mua card điện thoại rồi nhắn mã số cho người bán pháo trên mạng để mua pháo về đốt.

Hỏi: Việc A lên mạng xã hội mua pháo có đúng không?, vì sao?

Gợi ý trả lời:

Hành vi của người bán pháo cũng như của A là vi phạm pháp luật, vì theo Điểm d Khoản 1 Điều 18 Luật An ninh mạng thì hành vi Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật là vi phạm pháp luật.

Hành vi của A sẽ bị xử lý: Phạt tiền từ 5 đến 10 triệu đồng về hành vi Sản xuất, tàng trữ, mua, bán, vận chuyển trái phép pháo, thuốc pháo và đồ chơi nguy hiểm (Nghị định 167/2013/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy và chữa cháy; phòng, chống bạo lực gia đình)