BÁO CÁO BÀI TẬP

**Môn học: An toàn mạng – NT140.O11.ANTT**

**Tên chủ đề: Computer Security Concepts and Principles**

*GV: Nghi Hoàng Khoa*

**Nhóm: 13**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT140.O11.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 01 | Đinh Bùi Huy Phương | 21520090 | 21520090@gm.uit.edu.vn |
| 02 | Nguyễn Thị Thanh Mai | 21521112 | 21521112@gm.uit.edu.vn |
| 03 | Lê Đoàn Trà My | 21521149 | 21521149@gm.uit.edu.vn |
| 04 | Nguyễn Phương Trinh | 21521581 | 21521581@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung |  | Trang |
| 01 | Tóm tắt tất cả các Nguyên tắc Thiết kế Bảo mật (Security Design Principles) và đưa ra ví dụ cho từng nguyên tắc | | 02-04 |
| 02 | Hãy xem xét mã nguồn và trả lời câu hỏi | | 04 |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**Câu 01:** Tóm tắt tất cả các Nguyên tắc Thiết kế Bảo mật (Security Design Principles) và đưa ra ví dụ cho từng nguyên tắc.

→ Trả lời:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Nguyên tắc** | **Tóm tắt** | **Ví dụ** |
| 01 | Economy of mechanism  (Tính kinh tế của cơ chế) | Thiết kế biện pháp bảo mật nên đơn giản và nhỏ gọn nhằm tối thiểu hóa khả năng lỗi và yêu cầu bảo trì.  *(Nó đảm bảo việc kiểm tra, cập nhật dễ dàng hơn và giảm khả năng bị tấn công từ các lỗ hổng phức tạp)* | Thay vì một quá trình xác thực phức tạp thì hệ thống có thể chỉ cần 1 cặp (tài khoản, mật khẩu) để đăng nhập. |
| 02 | Fail-safe defaults  (Mặc định không an toàn) | Bất cứ khi nào quyền truy cập, đặc quyền / quyền hoặc một số thuộc tính liên quan đến bảo mật không được cấp rõ ràng, nó sẽ không được cấp quyền truy cập cho đối tượng đó. | Khi thêm user mới vào hệ điều hành, nhóm user mặc định có ít quyền truy cập vào tệp và dịch vụ hơn. |
| 03 | Complete mediation  (Dàn xếp hoàn toàn) | Mọi quyền truy cập phải được kiểm tra thông qua cơ chế kiểm soát truy cập. Không quyết định dựa vào các quyết định trước đó lấy từ cache. | Trang web/app ngân hàng yêu cầu người dùng đăng nhập lại sau một khoảng thời gian nhất định. |
| 04 | Open design  (Thiết kế mở) | Thiết kế, mã nguồn hệ thống bảo mật nên được công khai, cho phép đánh giá và xem xét công khai từ cộng đồng chuyên gia. | Hệ thống mã hóa mã nguồn mở (open-source encryption system). VD: GnuPG (GNU Privacy Guard), một phần mềm mã hóa và chữ ký số miễn phí và mã nguồn mở |
| 05 | Separation of privilege  (Phân chia đặc quyền) | Phân chia tài nguyên, đặc quyền kiểm soát của một hệ thống lớn nhằm giảm thiểu thiệt hại nếu bị tấn công.  *(Hệ thống cấp quyền truy cập dựa trên nhiều hơn một điều kiện được đáp ứng)* | Khi thực hiện chuyển tiền trực tuyến, cần user-id, mật khẩu và OTP. |
| 06 | Least privilege  (Đặc quyền tối thiểu) | Không cung cấp đặc quyền nhiều hơn những gì mà đối tượng (tiến trình/người dùng) cần để hoàn thành nhiệm vụ. | Hầu hết người dùng hệ thống không cần quyền root cho công việc hàng ngày. Chỉ cấp quyền root cho người có nhu cầu thực sự và có kiến thức |
| 07 | Least common mechanism  (Cơ chế ít phổ biến nhất) | Tài nguyên cần được chia sẻ tới ít bên nhất có thể | Thông tin của 1 sinh viên UIT chỉ có sinh viên đó và các giảng viên phòng ban UIT (CTSV, ĐTĐH) có thẩm quyền truy cập |
| 08 | Psychological acceptability  (Tâm lý chấp nhận) | Các biện pháp bảo mật không nên gây ảnh hưởng tới quá trình làm việc của người dùng, đồng thời phải minh bạch, cung cấp công cụ bảo mật cần thiết | Khi mật khẩu mới bị từ chối trong quá trình thay đổi, chương trình nêu rõ lý do tại sao mật khẩu bị từ chối thay vì đưa ra một thông báo lỗi khó hiểu hay không báo. |
| 09 | Isolation  (Cô lập) | Cô lập hệ thống, dữ liệu công cộng với dữ liệu mật; cô lập tiến trình và dữ liệu giữa các người dùng; cô lập cơ chế bảo mật với hệ thống bên ngoài, không cho truy cập trái phép vào các thành phần đó. | Có một mạng nội bộ công ty và muốn cô lập các máy tính của nhân viên khỏi mạng khách bằng cách cài đặt các thiết bị tường lửa và phân đoạn mạng tạo ra hai mạng con riêng biệt. |
| 10 | Encapsulation  (Đóng gói) | Một dạng cô lập cụ thể dựa trên hướng đối tượng. Đặt các quy trình và dữ liệu liên quan vào một miền riêng biệt, nơi chỉ có các quy trình bên trong miền và các điểm nhập miền chỉ định mới có thể truy cập. | Trong lập trình hướng đối tượng, chúng ta sử dụng các khái niệm như lớp, đối tượng và phạm vi truy cập để đóng gói và che giấu thông tin quan trọng. |
| 11 | Modularitzy  (Modul hoá) | Thiết kế và sử dụng các Modul cơ chế bảo mật độc lập, riêng lẻ. | Một ứng dụng web có tính năng đăng nhập và quản lý thông tin người dùng có thể có các modul: Xác thực, quản lý phiên, kiểm soát truy cập, mã hoá. |
| 12 | Layering  (Xếp lớp) | Sử dụng nhiều lớp bảo mật cho cùng một mục đích. | Hệ thống mạng nội bộ của một công ty với mục tiêu bảo vệ dữ liệu quan trọng. Hệ thống có thể gồm các lớp: firewall, hệ thống xác thực và quản lý quyền truy cập, hệ thống phát hiện xâm nhập, mã hoá dữ liệu lưu trữ riêng biệt. |
| 13 | Least astonishment  (Ít ngạc nhiên nhất) | Các chương trình và giao diện nên dễ hiểu và phản hồi các thao tác của người dùng một cách hợp lý. | Khi người dùng nhập thông tin đăng nhập của mình vào hệ thống, hệ thống nên đưa ra thông báo rõ ràng và chính xác về việc xác thực thành công hoặc thất bại. |

**Câu 02:** Hãy xem xét mã nguồn sau đây để cho phép truy cập vào một tài nguyên:

A black text on a white background

Description automatically generated

a. Giải thích lỗi bảo mật trong chương trình này.

→ Trả lời: Chương trình chưa đáp ứng Nguyên tắc Thiết kế Bảo mật "fail-safe default". Mặc định của đoạn chương trình trên là cho phép truy cập nên nếu hàm \*IsAccessAllowed()\* bị lỗi và trả về cho phép thì sẽ khó phát hiện được kịp thời. Chương trình nên mặc định không cung cấp quyền truy cập vì sẽ dễ sửa, thêm điều kiện truy cập mới hơn nghĩ ra các trường hợp để loại trừ truy cập trái phép.

b. Viết lại mã để tránh lỗ hổng.

→ Trả lời:

DWORD dwRet = IsAccessAllowed(...);

        if (dwRet == ACCESS\_ADMIN){

            //Security check OK.

            //Admin privilege

        }else if (dwRet == ACCESS\_STAFF){

            //Security check OK.

            //Staff privilege

        }else{

            //Security check failed.

            //Inform user that access is denied

        }

**\*THAM KHẢO**

1. Stallings William, Lawrie Browm. Section 1.4, Chap 1, Computer Security.

2. Fundamental Security Design Principles, <https://binaryterms.com/fundamental-security-design-principles.html>.

3. Nguyên tắc của an ninh mạng, <https://websitehcm.com/nguyen-tac-cua-an-ninh-mang/>.

4. Design Principles, <https://www.cs.clemson.edu/course/cpsc420/material/Design%20Principles/Design%20Principles.pdf> .

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)