Họ tên: Phạm Thùy Trang

Lớp: 10DH\_CNPM2

MSSV: 1050080159

**LAB 2**

1.

A screenshot of a computer monitor

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Sau quá trình thực hành, sinh viên trả lời các câu hỏi sau:

1. Nêu biện pháp phòng tránh; các cách phát hiện Keylogger trên máy tính - điện

thoại và minh họa nếu có thể.

**Biện pháp phòng tránh Keylogger**

* Không tải phần mềm không rõ nguồn gốc: Chỉ cài đặt ứng dụng từ các trang web chính thống như Microsoft Store, Google Play, App Store.
* Sử dụng phần mềm diệt virus: Các phần mềm như Kaspersky, Bitdefender, Norton có thể giúp phát hiện và tiêu diệt keylogger.
* Bật xác thực hai yếu tố (2FA): Ngay cả khi bị đánh cắp mật khẩu, hacker vẫn không thể đăng nhập mà không có mã xác thực.
* Sử dụng bàn phím ảo: Khi nhập thông tin nhạy cảm như mật khẩu, hãy dùng bàn phím ảo để tránh bị ghi lại.
* Cập nhật hệ điều hành và phần mềm: Vá lỗi bảo mật giúp ngăn chặn các lỗ hổng mà hacker có thể khai thác.
* Không nhấp vào liên kết lạ: Keylogger có thể lây nhiễm qua email giả mạo hoặc trang web không an toàn.
* Giới hạn quyền ứng dụng: Trên điện thoại, hạn chế quyền truy cập của ứng dụng vào bàn phím và hệ thống.

**Cách phát hiện Keylogger**

**Trên máy tính**

1. **Kiểm tra Task Manager**

* Nhấn Ctrl + Shift + Esc → Chuyển sang tab **Processes** → Tìm các tiến trình lạ tiêu tốn CPU/RAM cao.

1. **Sử dụng công cụ Windows Defender hoặc phần mềm diệt virus**

* Chạy quét toàn bộ hệ thống để phát hiện phần mềm độc hại.

1. **Kiểm tra các chương trình khởi động cùng Windows**

* Nhấn Win + R → nhập msconfig → Tab **Startup** → Xem có chương trình lạ không.

1. **Kiểm tra kết nối mạng**

* Mở Command Prompt (cmd) → nhập netstat -ano để kiểm tra các kết nối bất thường.

1. **Sử dụng phần mềm quét chuyên dụng**

* Spybot - Search & Destroy, Malwarebytes có thể tìm và gỡ bỏ keylogger.

**Trên điện thoại**

1. **Kiểm tra ứng dụng đang chạy**

* Vào **Cài đặt** → **Ứng dụng** → Xem danh sách các ứng dụng chạy nền lạ.

1. **Quét bằng phần mềm bảo mật**

* Dùng Kaspersky Mobile, Avast Mobile Security để quét virus.

1. **Xem quyền truy cập ứng dụng**

* Kiểm tra ứng dụng nào đang có quyền truy cập bàn phím, tin nhắn, ghi âm…

1. **Kiểm tra mức sử dụng dữ liệu**

* Nếu có ứng dụng nào sử dụng dữ liệu đột biến mà bạn không dùng, có thể là Keylogger gửi dữ liệu ra ngoài.

**2. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính và điện thoại khác.**

**Keylogger trên máy tính**

1. **Spyrix Free Keylogger**

* Ghi lại tất cả thao tác nhập từ bàn phím, chụp ảnh màn hình, theo dõi clipboard.
* Ẩn hoàn toàn trong hệ thống, khó phát hiện nếu không dùng phần mềm bảo mật.

1. **Elite Keylogger**

* Tự động gửi báo cáo qua email, theo dõi mật khẩu và tin nhắn trên trình duyệt.

1. **Revealer Keylogger**

* Chụp ảnh màn hình khi người dùng nhập dữ liệu, ghi lại bàn phím và clipboard.

**B. Keylogger trên điện thoại**

1. **FlexiSPY**

* Ghi lại bàn phím, tin nhắn SMS, cuộc gọi và cả âm thanh môi trường xung quanh.
* Chạy ẩn, rất khó phát hiện nếu không có phần mềm bảo mật.

1. **MSpy**

* Theo dõi tin nhắn, email, bàn phím, và lịch sử duyệt web trên điện thoại.

1. **KidLogger**

* Theo dõi hoạt động điện thoại của trẻ em, nhưng có thể bị kẻ xấu lợi dụng làm keylogger.