**DEMO AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN**

1. **Demo tấn công.**

**Demo 1: Tài khoản ẩn window**

**Mô tả:**

Mô phỏng một cuộc tấn công sử dụng BadUSB (Arduino) để tự động tạo một tài khoản người dùng ẩn trên hệ thống Windows. Tài khoản này không hiển thị trong giao diện thông thường và có thể được kẻ tấn công sử dụng để chiếm quyền điều khiển máy tính hoặc đánh cắp dữ liệu mà người dùng không hề hay biết.

**Công cụ và môi trường:**

* Arduino Board: Một thiết bị giả lập bàn phím sử dụng mạch Ardunino.
* Arduino IDE: Phần mềm dùng để lập trình và nạp mã vào Arduino.
* Máy mục tiêu: Hệ điều hành Windows (phiên bản bất kỳ).

**Quy trình Demo:**

Bước 1: Lập trình Payload để tạo tài khoản ẩn trong Windows.

Bước 2: Mở Arduino IDE, nạp đoạn mã Demo1.txt vào board Arduino.

Bước 3: Cắm Arduino vào cổng USB của máy mục tiêu. Arduino sẽ giả lập bàn phím, tự động thực thi lệnh trong Command Prompt để tạo tài khoản ẩn.

Bước 4: Kiểm tra kết quả bằng cách mở Command Prompt trên máy nạn nhân và chạy lệnh:

**net user**

Kết quả là tài khoản hiddenuser sẽ không xuất hiện trong danh sách người dùng thông thường.

**Demo 2: Tạo revershell**

A diagram of a computer system

Description automatically generated  
**Mô tả:**

Mô phỏng một cuộc tấn công sử dụng **BadUSB** để tạo một **Reverse Shell** kết nối từ máy mục tiêu về máy tấn công. Cuộc tấn công này minh họa cách một thiết bị USB giả mạo có thể được lập trình để thực thi mã độc và chiếm quyền điều khiển từ xa trên hệ thống.

**Công cụ và môi trường:**

* BadUSB: Thiết bị USB giả lập bàn phím bằng cách sử dụng mạch Arduino
* Máy tấn công: Hệ điều hành Kali Linux hoặc bất kỳ hệ điều hành nào có cài đặt netcat.
* Máy mục tiêu: Hệ điều hành Windows (phiên bản có sẵn terminal hoặc PowerShell).
* Phần mềm hỗ trợ:
  + Netcat (nc): Được dùng trên máy tấn công để lắng nghe kết nối.
  + Arduino IDE: Phần mềm sử dụng để nạp mã độc vào Arduino.

**Quy trình Demo:**

Bước 1: Tạo tập lệnh giả lập bàn phím tự động nhập các lệnh để thiết lập reverse shell.

Bước 2: Sử dụng Ardunio IDE để nạp tập lệnh Demo2.txt đã tạo vào BadUSB.

Bước 3: Thiết lập Listener trên máy tấn công bằng cách chạy lệnh sau để lắng nghe kết nối từ máy nạn nhân:

**stty raw -echo; (stty size; cat) | nc -lvnp 246 -k**

* stty raw -echo: Đây là một lệnh để cài đặt chế độ giao tiếp của thiết bị. Trong trường hợp này, raw được sử dụng để thiết lập chế độ đọc dữ liệu mà không thực hiện bất kỳ xử lý nào (như tùy chỉnh hoặc biến đổi dữ liệu).
* -echo tắt chức năng echo, nghĩa là không hiển thị dữ liệu nhận được trên terminal.
* Kết quả là, dòng lệnh này thiết lập một kết nối TCP server trên cổng 81 và đọc dữ liệu từ client kết nối tới, trong khi không hiển thị dữ liệu nhận được trên terminal.
* |: Đây là toán tử pipe, được sử dụng để chuyển đầu ra của lệnh trước (stty size; cat) thành đầu vào của lệnh sau (nc -lvnp 81 -k).

Bước 4: Cắm BadUSB vào máy nạn nhân. Khi cắm vào, BadUSB sẽ giả lập bàn phím và tự động nhập các lệnh payload lên PowerShell hoặc Terminal. Máy nạn nhân sẽ khởi tạo một phiên kết nối từ xa (reverse shell) về máy tấn công.

Bước 5: Khi payload chạy thành công, máy tấn công sẽ nhận được một phiên shell từ máy mục tiêu thông qua netcat.

Ví dụ:

PS C:\Users\Victim> whoami

victim\administrator

**Demo 3: Lấy mật khẩu wifi của nạn nhân.**

**Mô tả:**

Mô phỏng một cuộc tấn công thu thập mật khẩu Wi-Fi đã được lưu trên máy tính của nạn nhân bằng cách sử dụng lệnh hệ thống kết hợp với BadUSB. Cuộc tấn công minh họa cách một thiết bị giả lập bàn phím tự động hóa quá trình trích xuất thông tin mạng Wi-Fi và gửi thông tin đến máy tấn công bằng email.

**Công cụ và môi trường:**

* BadUSB: Thiết bị USB giả lập bàn phím bằng cách sử dụng mạch Arduino.
* Máy mục tiêu: Máy tính Windows của nạn nhân, có lưu trữ mật khẩu Wi-Fi.
* Máy tấn công: Nhận email chứa thông tin Wi-Fi từ máy nạn nhân.

**Quy trình Demo:**

Bước 1: Tạo tập lệnh giả lập bàn phím tự động nhập các lệnh để thiết lập reverse shell.

Bước 2: Sử dụng Ardunio IDE để nạp tập lệnh Demo3.txt đã tạo vào BadUSB.

Bước 3: Cắm BadUSB vào máy nạn nhân. Khi cắm vào, BadUSB sẽ giả lập bàn phím và tự động nhập các lệnh payload lên PowerShell hoặc Terminal. Máy nạn nhân sẽ tự gửi thông tin mật khẩu Wi Fi đến máy tấn công vã xoá sạch mọi dấu vết.

Bước 4: Kiểm tra mail đã được cấu hình để lấy được thông tin mật khẩu Wifi của nạn nhân đã được lưu trong máy.

1. **Demo phòng chống.**

**Demo 1: Chặn cổng USB.**

**Mô tả:**

Minh họa cách chặn cổng USB để ngăn chặn các thiết bị không được phép, như BadUSB hoặc USB chứa mã độc, từ đó phòng ngừa các cuộc tấn công tự động hóa như tạo tài khoản ẩn, lấy mật khẩu Wi-Fi hoặc chiếm quyền điều khiển hệ thống.

**Công cụ và môi trường:**

* Máy tính mục tiêu: Hệ điều hành Windows.
* Quyền quản trị viên: Cần có quyền để chỉnh sửa cài đặt hệ thống.

**Quy trình Demo:**

Bước 1: Mở Device Manager và tiến hành tắt Driver của cổng USB.

Bước 2: Cắm BadUSB chứa bất kỳ mã độc trong các Demo tấn công ở trên vào.

Bước 3: Kiểm tra thấy máy không nhận lệnh từ BadUSB nữa.

**Demo 2: Khoá máy khi đi ra ngoài.**

**Mô tả:**

Minh họa cách khóa máy tính khi rời khỏi vị trí để bảo vệ máy tính khỏi các cuộc tấn công vật lý, chẳng hạn như cắm thiết bị BadUSB vào máy hoặc truy cập dữ liệu trái phép.

**Công cụ và môi trường:**

* Máy tính mục tiêu: Hệ điều hành Windows và có cài đặt mật khẩu màn hình.

**Quy trình Demo:**

Bước 1: Nhấn tổ hợp phím Windows + L hoặc chọn Lock trong menu Start.

Bước 2: Cắm BadUSB chứa bất kỳ mã độc trong các Demo tấn công ở trên vào.

Bước 3: Kiểm tra thấy máy vẫn nhận lệnh từ BabUSB nhưng không thể truy cập vào trong và mở bất kỳ ứng dụng nào lên.