

《職業駭客的修練》

图书基本信息

书名：《職業駭客的修練》

13位ISBN编号：978986434157X

出版时间：2016-10-31

作者：秋聲

页数：304

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《職業駭客的修練》

內容概要

這是一本寫給程式設計師的，也是寫給想成為職業駭客的書。因此，本書採用程式設計師最熟悉的開發環境Visual Studio作為反組譯的工具。本書會以C語言的程式為例，編譯後再反組譯，一步一步教會您如何解析機器碼對應的組合語言，找出程式的關鍵之處，透過特定的手法來破解程式，例如略過密碼檢查、修改遊戲金幣等等。此外，考量到駭客的實際工作環境，也會對於Windows PE進行初步的介紹。

《職業駭客的修練》

作者簡介

秋聲
浪蕩漂泊十載有餘，偶然間面海時忽得一悟：
原來自身興趣在底層。
愛旅行，曾被醫生宣告患上「不去旅行會死症」的症狀，至今仍無藥可醫；更熱愛技術，尤其是底層的駭客技術；也愛學語言，目前正在研習第三外國語，目的是希望有朝一日能往北歐國家旅行去。
目前隱居中從事作家的的工作，與室友還有他的兩隻貓共同生活在同一個屋簷下。

書籍目錄

機器碼：C 語言把玩篇

Chapter 1 C 語言程式的基本結構

1.1 啼聲初開

Chapter 2 HelloWorld

2.1 HelloWorld的基本結構

2.2 HelloWorld的運行過程

2.3 小結論

Chapter 3 對HelloWorld 來做修改

3.1 起頭

3.2 修改記憶體位址當中的機械碼-文字篇

3.3 修改push字串的位址

3.4 黑掉機械碼

Chapter 4 加法程式的運作原理

4.1 簡單的加法程式-賦值

4.2 簡單的加法程式-運算

Chapter 5 熱身總結

5.1 開場白的前戲

5.2 猜想的藝術-猜想機械碼的意義

5.3 解開機械碼的意義

5.4 逐步執行

Chapter 6 邏輯判斷式

6.1 邏輯判斷式的基礎-if

6.2 比出jle 的操作碼

6.3 作業

6.4 補充

Chapter 7 循環

7.1 for 循環的特徵

7.2 偏移量的算法

7.3 作業

Chapter 8 趣味應用- 修改遊戲金幣

8.1 利用for 循環來設計遊戲- 只玩五次的情況

8.2 利用機械碼來修改遊戲- 把只玩五次的遊戲修改成玩十次

Chapter 9 被呼叫函數的位址換算

9.1 位址找尋

9.2 作業

Chapter 10 編譯器堆疊- 帶參數的堆疊變化實戰篇

10.1 簡單的堆疊實例

10.2 堆疊實例的研討

Chapter 11 修改被呼叫函數的妙招

Chapter 12 陣列

12.1 變數賦值

12.2 陣列賦值

Chapter 13 指標

13.1 指標的基本入門-單指標

13.2 找出指標以及指標裡頭的位址

13.3 多重指標

13.4 改變指標的指向

Chapter 14 綜合作業-結構

底層：Windows PE 把玩篇

Chapter 15 可執行檔的入口點

15.1 使用Visual Studio 來觀察可執行檔的入口點

15.2 使用PEview 來觀察可執行檔的入口點

Chapter 16 找出定義PE 的文件以及定義範圍

Chapter 17 C 語言當中的結構設計簡介

17.1 結構最簡單的寫法

17.2 雙變數的結構

17.3 結構中放置不同變數的情況

17.4 雙重結構

Chapter 18 PE 的範圍以及PE-IMAGE_DOS_HEADER 的元素

18.1 PE 的範圍

18.2 PE-IMAGE_DOS_HEADER 的元素

Chapter 19 PE-IMAGE_NT_HEADERS

Chapter 20 綜合研究- 對PE 加殼前與加殼後的機械碼比較

Appendix A 組合語言機械碼對照表

《職業駭客的修練》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com