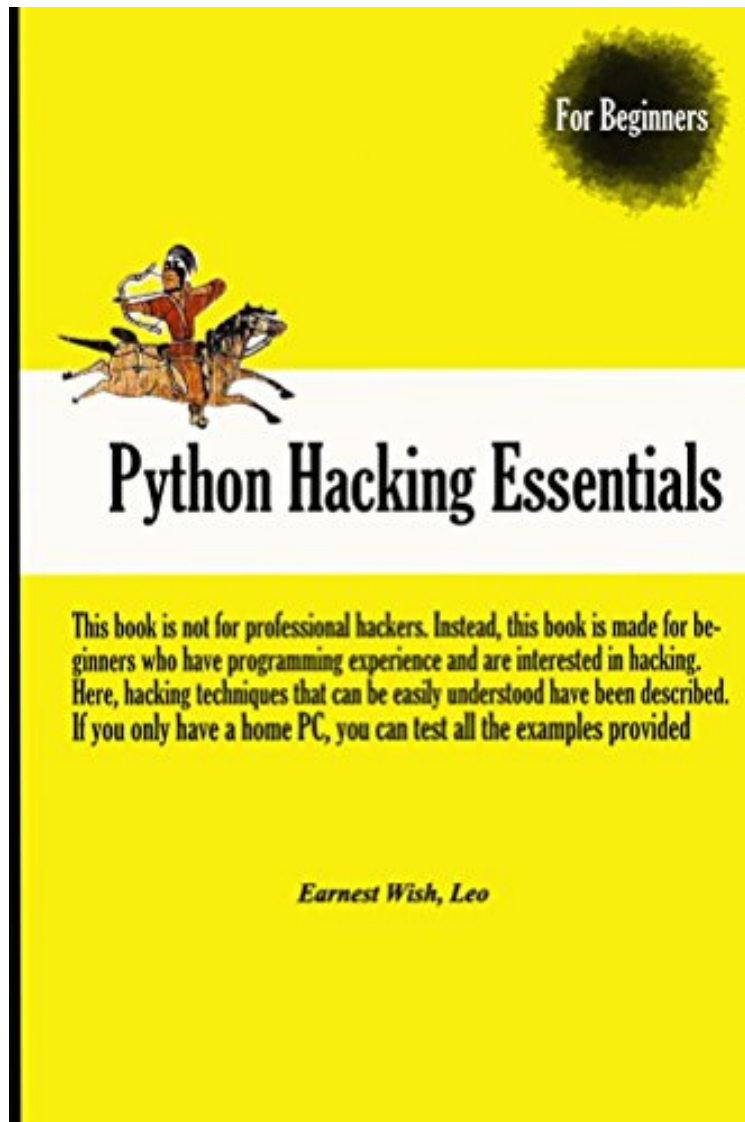


[Mobile ebook] Python Hacking Essentials (English Edition)

## Python Hacking Essentials (English Edition)

*Von Earnest Wish, Leo*

*DOC | \*audiobook | ebooks | Download PDF | ePub*



DOWNLOAD



READ ONLINE

Produktinformation -Verkaufsrank: #594772 in eBooksVerffentlicht am: 2015-04-20Erscheinungsdatum: 2015-04-20File Name: B00WFP9S2E | File size: 50.Mb

**Von Earnest Wish, Leo : Python Hacking Essentials (English Edition)** before purchasing it in order to gage whether or not it would be worth my time, and all praised Python Hacking Essentials (English Edition):

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. Python 2.xVon CustomerBasiert noch auf Python 2.x... damit ist schon fast alles zu dem Buch gesagt.Aufmachung und Satz

sind auch eher mau, in Summe wrde ich 2,5 Sterne vergeben mit dem Prdikat "geht so"

**Kurzbeschreibung**  
**Target Audience** This book is not for professional hackers. Instead, this book is made for beginners who have programming experience and are interested in hacking. Here, hacking techniques that can be easily understood have been described. If you only have a home PC, you can test all the examples provided here. I have included many figures that are intuitively understandable rather than a litany of explanations. Therefore, it is possible to gain some practical experience while hacking, since I have only used examples that can actually be implemented. This book is therefore necessary for ordinary people who have a curiosity of hackers and are interested in computers.

**Organization of the Book** This book is made up of five major parts, from basic knowledge to actual hacking code. A beginner is naturally expected to become a hacker while reading this book.

**Hacking Preparation** Briefly introduce the basic Python syntax that is necessary for hacking.

**Application Hacking** Introduce the basic skills to hack an application, such as Keyboard hooking, API hooking and image file hacking.

**Web Hacking** The Virtual Box test environment configuration is used for a Web Shell attack to introduce web hacking, which is currently an important issue. The techniques include SQL Injection, Password Cracking, and a Web Shell Attack.

**Network Hacking** A variety of tools and the Python language can be combined to support network hacking and to introduce the network hacking technique. Briefly, we introduce NMap with the Wireshark tool, and hacking techniques such as Port Scanning, Packet Sniffing, TCP SYN Flood, Slowris Attack are introduced.

**System Hacking** System hacking is difficult to understand for beginners, and in this section, figures are used to introduce difficult concepts. The hacking techniques that are introduced include a Backdoor, Registry Handling, Stack Based Buffer Overflow, and SEH Based Buffer Overflow.

While reading this book, it is possible to obtain answers for such problems one by one. After reading the last chapter, you will gain the confidence to be a hacker.

**Features of this book** When you start to study hacking, the most difficult task is to configure the test environment. There are many problems that need to be addressed, such as choosing from the variety in operating systems, obtaining expensive equipment and using complex technology. Such problems are too difficult to take in at once, so this book overcomes this difficulty by implementing a simple idea.

First, systems will be described as Windows-based. We are very familiar with Windows, so it is very easy to understand a description based on Windows. Since Windows, Linux, Unix, and Android are all operating systems, it is possible to expand the concepts that are discussed here.

Second, we use a virtual machine called Virtual Box. For hacking, it is necessary to connect at least three or more computers on a network. Since it is a significant investment to buy a few computers only to study these techniques, a virtual machine can be used instead to easily implement a honeypot necessary to hack by creating multiple virtual machines on a single PC.

Finally, abstract concepts are explained using figures. Rather than simply using words for descriptions, graphics are very effective in transferring information. An abstract concept can materialize through the use of graphics in order to improve the understanding on the part of the reader.

**Kurzbeschreibung**  
**Target Audience** This book is not for professional hackers. Instead, this book is made for beginners who have programming experience and are interested in hacking. Here, hacking techniques that can be easily understood have been described. If you only have a home PC, you can test all the examples provided here. I have included many figures that are intuitively understandable rather than a litany of explanations. Therefore, it is possible to gain some practical experience while hacking, since I have only used examples that can actually be implemented. This book is therefore necessary for ordinary people who have a curiosity of hackers and are interested in computers.

**Organization of the Book** This book is made up of five major parts, from basic knowledge to actual hacking code. A beginner is naturally expected to become a hacker while reading this book.

**Hacking Preparation** Briefly introduce the basic Python syntax that is necessary for hacking.

**Application Hacking** Introduce the basic skills to hack an application, such as Keyboard hooking, API hooking and image file hacking.

**Web Hacking** The Virtual Box test environment configuration is used for a Web Shell attack to introduce web hacking, which is currently an important issue. The techniques include SQL Injection, Password Cracking, and a Web Shell Attack.

**Network Hacking** A variety of tools and the Python language can be combined to support network hacking and to introduce the network hacking technique. Briefly, we introduce NMap with the Wireshark tool, and hacking techniques such as Port Scanning, Packet Sniffing, TCP SYN Flood, Slowris Attack are introduced.

**System Hacking** System hacking is difficult to understand for beginners, and in this section, figures are used to introduce difficult concepts. The hacking techniques that are introduced include a Backdoor, Registry Handling, Stack Based Buffer Overflow, and SEH Based Buffer Overflow.

While reading this book, it is possible to obtain answers for such problems one by one. After reading the last chapter, you will gain the confidence to be a hacker.

**Features of this book** When you start to study hacking, the most difficult task is to configure the test environment. There are many problems that need to be addressed, such as choosing from the variety in operating systems, obtaining expensive equipment and using complex technology. Such problems are too difficult to take in at once, so this book overcomes this difficulty by implementing a simple idea.

First, systems will be described as Windows-based. We are very familiar with Windows, so it is very easy to understand a description based on Windows. Since Windows, Linux, Unix, and Android are all operating systems, it is

possible to expand the concepts that are discussed here. Second, we use a virtual machine called Virtual Box. For hacking, it is necessary to connect at least three or more computers on a network. Since it is a significant investment to buy a few computers only to study these techniques, a virtual machine can be used instead to easily implement a honeypot necessary to hack by creating multiple virtual machines on a single PC. Finally, abstract concepts are explained using figures. Rather than simply using words for descriptions, graphics are very effective in transferring information. An abstract concept can materialize through the use of graphics in order to improve the understanding on the part of the reader.

ber den Autor und weitere Mitwirkende Earnest Wish has 15 years of experience as an information security professional and a white hacker. He developed the internet stock trading system at Samsung SDS at the beginning of his IT career, and he gained an extensive amount experience in hacking and security while operating the Internet portal system at KTH (Korea Telecom Hitel). He is currently responsible for privacy and information security work in public institutions and has deep knowledge with respect to vulnerability assessments, programming and penetration testing. He obtained the Comptia Network + Certification and the license of Professional Engineer for Computer System Applications. This license is provided by the Republic of Korea to leading IT Professionals. Leo is a computer architect and a parallel processing expert. He is the author of six programming books. As a junior programmer, he developed a billing system and a hacking tool prevention system in China. In recent years, he has studied security vulnerability analysis and the improvement in measures for parallel programming. Now, he is a lead optimization engineer to improve CPU and GPU performance.