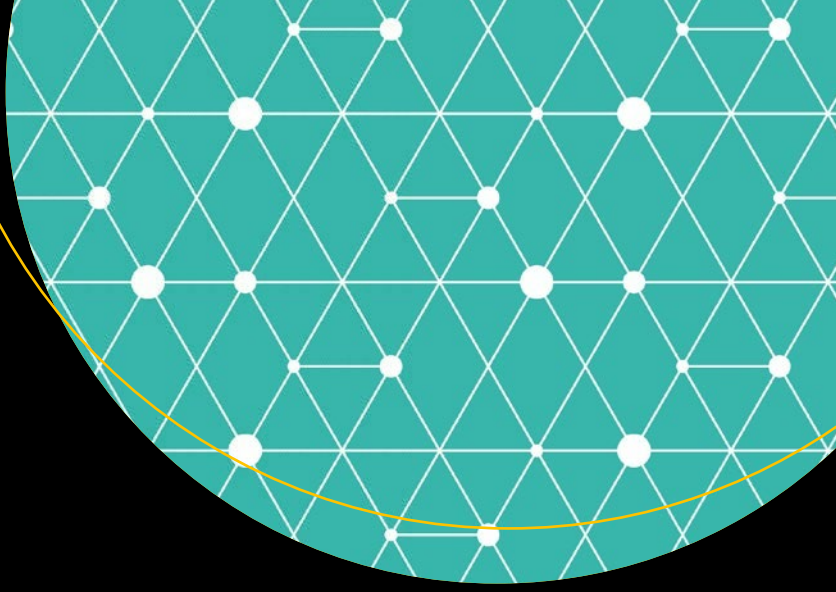

Beginning Ethical Hacking with Python

Sanjib Sinha

Apress®

Beginning Ethical Hacking with Python

Sanjib Sinha

Apress®

Beginning Ethical Hacking with Python

Sanjib Sinha
Howrah, West Bengal, India

ISBN-13 (pbk): 978-1-4842-2540-0 ISBN-13 (electronic): 978-1-4842-2541-7

DOI 10.1007/978-1-4842-2541-7

Library of Congress Control Number: 2016963222

Managing Director: Welmoed Spahr
Lead Editor: Nikhil Karkal
Technical Reviewer: Abir Ranjan Atarthy
Editorial Board: Steve Anglin, Pramila Balan, Laura Berendson, Aaron Black, Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Nikhil Karkal, James Markham, Susan McDermott, Matthew Moodie, Natalie Pao, Gwenan Spearing
Coordinating Editor: Prachi Mehta
Copy Editor: Larissa Shmailo
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text are available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/. Readers can also access source code at SpringerLink in the Supplementary Material section for each chapter.

Printed on acid-free paper

DR. AVIJIT SEN, DRISTIPRADIP, KOLKATA.

(For Bringing Light into Darkness)

Contents at a Glance

Contents

About the Author

Sanjib Sinha writes stories and codes—not always in the same order.

He started with C# and .NET framework and won a Microsoft Community Contributor Award in 2011. Later, the Open Source Software movement attracted him and he became a Linux, PHP, and Python enthusiast, specializing in and working on White Hat Ethical Hacking.

As a beginner, he had to struggle a lot—always—to find out an easy way to learn coding. No one told him that coding is like writing: imagining an image and bringing it down to Earth with the help of words and symbols.

All through his books he has tried to help beginners from their perspective—as a beginner.

About the Technical Reviewer

Abir Ranjan Atarthy is a Certified Ethical Hacker from Ec-Council, ISO27001 Auditor and PCIDSS implementer.

He has more than 12 years of extensive domain experience in driving the Information & Cyber Security programs in all key aspects i.e. Policy, Standards, Procedures, Awareness, Network Security, Web security, Android App Security, Incident Response, Security Analytics, Security Monitoring, Malware protection, Security configuration, Cryptography, Data Protection Knowledge of most advanced tools in security industry with complementing knowledge on scripting languages to manually exploit vulnerabilities.

He has authored several technical articles which have been published in IT security journals and is frequently invited to speak at many cyber security conferences and Python forums.

He has designed cyber security courses for Corporates on network and web penetration testing, forensics, and cryptography.

Abir regularly conducts work-shops, training sessions and certification programs for corporates, government organizations, defence establishments, security agencies, engineering colleges and universities on Python programming, penetration testing and cyber forensics.

He has created several IT security and cryptographic tools using Python.

He has accomplished short term Programs in Object-oriented programming and Selected Topics in Software Engineering from Indian Institute of Technology -Kharagpur.

Abir is considered a subject-matter expert in cyber security and is often quoted by leading newspapers and TV channels.

Presently he is leading the Cyber threat intelligence department in TCG Digital Solutions Pvt. Ltd.

Acknowledgments

KARTICK PAUL, SYSTEM MANAGER, AAJKAAL, KOLKATA, Without his persistent and inspiring help, I could not write this book.

Prologue – Hacker's Goal

This book is intended for complete programming beginners or general people who know nothing about any programming language but want to learn ethical hacking.

Let us clear it first: Ethical Hacking is not associated with any kind of illegal electronic activities. They always stay within laws. This book is intended for those people – young and old – who are creative and curious and who want to develop a creative hobby or take up internet security profession acting as ethical hacker. Keeping that in mind we'll also learn Python 3 programming language to enhance our skill as ethical hackers.

This book is not intended for any kind of malicious user. If anyone tries to use this book or any type of code examples from this book for illegal purpose this book will take no moral responsibility for that malicious behaviours.

If you think that you can use this book for any malicious purpose then you are advised to read the first chapter "Legal Side of Ethical Hacking". I hope you won't like the idea of ending up in jail by harming some other systems.

I would like to start this brief introduction with an image. This image depicts many things that I will later discuss in detail. It says, "The author is using "Ubuntu" Linux distribution as his default operating system. He has installed Virtual Box – a kind of virtual machine – that runs in Windows also. And in that Virtual Box he has installed three more operating systems. One is "Windows XP" and the other two are "Kali Linux" and "Windows 7 Ultimate". The image also says, and that is very important, "Currently three operating systems are virtually running on the desktop".

(**The virtual Box is running three operating systems. You can try any kind of experiment on this Virtual OS. That will not damage your main system.**)

As an ethical hacker you will learn how to defend yourself. To defend yourself sometime you need to attack your enemy. But it is a part of your defense system. It is a part of your defense strategy. More you know about your enemy's strategy, more you can defend yourself. You need to learn those tools are frequently used by the malicious hackers or crackers. They use the same tool that you use to defend yourself.

Whether you are an ethical hacker or a malicious cracker, you do the same thing. You use the identical software tools to attack the security system. Only your purpose or intention differs.

Probably you know that a big car company before launching a new model of car generally tests the locking system. They have their own security engineers and besides they call for the locking experts to test the vulnerability. They pay a good amount of money if you can break the locking system of the car. Basically it is a work of "PENTESTING". The locking experts PENTESTS the system and see if there is any weakness in the system.

It is good example of ethical hacking. The locking experts are invited to do the job and they are paid well. On the contrary car thieves do the same job without any invitation. They simply break the locking system of an unattended car parked on the road side and take it away. I hope by now you have understood the difference between ethical hacking and cracking.

Your main intention centers on the security of the system. Security consists of four key components. As the book progresses you will increasingly be finding words like "PENTESTING", "EXPLOIT", "PENETRATION", "BREAK IN THE SYSTEM", "COMPROMISE THE ROUTER" etcetera. The four key components mentioned below mainly deal with these terms. The key components are:

1. Availability
2. Integrity
3. Authenticity
4. Confidentiality

We will see how crackers want to attack these components to gain access to the system. Since a hacker's main goal is to exploit the vulnerabilities of the system so he wants to see if there is any weakness in these core components.

Let us assume the hacker wants to block the availability of the data. In that case he will use the "Denial of Attack" or 'DoS' method. To do this attack usually hackers use system's resource or bandwidth. But DoS has many other forms. When the resource or bandwidth of your system is eaten up completely, the server usually crashes. The final target is one system but the number of victims is plenty. It is something like millions of people gather in front your house main door and jam it with a kind of human chain so that you and your family members can not enter into it.

The second key component Integrity should not be compromised at any cost. What does this term "integrity" mean? It's basically centered on the nature of data. When this nature of data is tampered with some kind of 'BIT-FLIPPING' attacks, the integrity of the system is also compromised. It can be done just by changing the message itself. The data may either be in the move or at rest, but it can be changed. Imagine what happens when a transaction of money is tampered with the addition of few more zeroes at the end! Let us assume a bank is transferring money. In its instruction it is written: "transfer $10, 000". Now the attacker changes the cryptic text in such a manner so that the amount changes to $10, 000000. So the attack is intended for the message itself or a series of messages.

The issue of authentication is normally handled by the Media Access Control (MAC) filtering. If it is properly placed the network does not allow unauthorized device. What happens if someone spoofs the MAC Address of a legitimate network station and takes it off? He can take on the station's identity and control it. This is called authentication attack or MAC Address spoofing.

Finally the issue of confidentiality rises above all. Data travel in clear text across the trusted network. Here data mean information. The information theft like cracking someone's password is confidentiality attack. The data or information is intended for someone but instead of the recipient the hacker gains the access. Actually the cracker steals it when the data is moving across the trusted network as clear text.

PART I

CHAPTER 1

Legal Side of Hacking

As time goes by and we progress, our old environment is also changing very fast. It has not been like before when we keep records by entering data into a big logbook and stack them one by one date-wise. Now we keep data in a computer. We don't go to a market anymore to buy anything. We order it over the Internet and payment is made by using credit or debit card. The nature of crime has also changed accordingly.

Criminals used to snatch your data physically before. They now snatch it over the Internet using computers. Now computers have become a new tool for business as well as for traditional crimes. On the basis of which, a term—"cyberlaw"—comes to the fore. As an ethical hacker, the first and most basic thing you should remember is "don't try to penetrate or tamper any other system without asking permission."

You may ask how I would experiment with my knowledge. The answer is Virtual Box. In your virtual machine you may install as many operating systems as you want and experiment on them (The above image depicts Virtual Box and two operating systems running in it). Try everything on them. Trying any virus on your virtual machine will not affect your main system. At the same time you will keep learning about malware, viruses and every kind of possible attack.

A few examples may give you an idea what type of computer crimes are punishable in our legal system.

If you use any software tool to generate a credit card or debit card number, then it is a highly punishable offense. It will invite a fine of fifty thousand dollars and fifteen years of imprisonment. Setting up a bogus web site to take credit card numbers with a false promise of selling non-existent products is a highly punishable offense. Rigorous imprisonment and a hefty fine follow. I can give you several other examples that may invite trouble for you if you don't stay within the law.

Remember, you are an ethical hacker and you are learning hacking tools for protecting your or your client's system. For the sake of protection and defense, you need to know the attack, exploit or penetration methods.

Try every single experiment on your virtual machine.

That is the rule number one of ethical hacking.

Electronic supplementary material The online version of this chapter (doi:10.1007/978-1-4842-2541-7_1) contains supplementary material, which is available to authorized users.

S. Sinha, *Beginning Ethical Hacking with Python*, DOI 10.1007/978-1-4842-2541-7_1

CHAPTER 2

Hacking Environment

The very first thing that you need is a virtual machine. As I said before, I have Ubuntu as my default operating system and inside my virtual machine I have installed two operating systems—one is Windows XP and the other is Kali Linux.

Technically, from now on I would mention Windows XP and Kali Linux as my virtual machines. Kali Linux is a Linux distribution that comes up with many useful hacking tools. So I strongly suggest using it as your virtual machine. You may also read the documentation page of Kali Linux, which will also be an immense help.

At the same time, I'd not suggest using Windows of any kind for the ethical hacking purpose. Some may argue that few hacking tools can be used in Windows, so why you are suggesting otherwise? The point is: in the ethical hacking world, you need to be anonymous all the time. You won't want to keep your trail, anyway, so that you can be traced back. Remaining anonymous is a big challenge. In Linux it is fairly easy and you can stay anonymous for the time being.

Keeping that in mind, I explain that technique of being anonymous in great detail so that before jumping up into the big task, you make your defense much stronger. Being anonymous is the most important thing in the world of ethical hacking. Keeping yourself anonymous in Windows is not possible. So it is better to adapt to the Linux environment first. Another important thing is, most of the great hacking tools are not available in the Windows environment.

If you have never heard of any Linux distribution, don't worry. You can either install user-friendly Ubuntu inside your Windows system or you can easily partition your disk into two parts and install Ubuntu and Windows separately as your two default operating systems. It is preferable to do the latter. Installing and uninstalling parallel operating systems always teaches you something new. If you are familiar with Windows, I won't tell you to simply dump it for the sake of learning ethical hacking. You can keep it and use it for your daily work. There is no problem in doing this.

In the Internet world, Linux is used more. So you need to learn a few Linux commands. Software installation in Linux is slightly different from Windows environments. There are Linux distributions like Fedora or Debian, and many more. I named Ubuntu just because it is extremely popular and Windows users find themselves comfortable inside it. The operations are more or less the same, including the software installations. For beginners, it is not a good idea to install Kali Linux as your default OS. You must read Kali documentation, where it is clearly stated that Kali is more for developers. You are going to install it inside your Virtual Box. Kali Linux is a kind of Linux distribution that comes with lot of hacking tools. You need to know them and use them in the course of ethical hacking.

S. Sinha, *Beginning Ethical Hacking with Python*, DOI 10.1007/978-1-4842-2541-7_2

Installing Virtual Machine is a very important step as the first step of building your environment. In the next chapter I will show you how you can do that for different operating systems. Another important thing is learning a programming language that will really help you learn ethical hacking better.

The obvious choice is Python. At the time of writing this book, Python 3.x has already arrived and is considered the future of this language. It is very quickly catching up with the old Python 2.x version, which has been around the market for a while. The official Python download page provides the repository of Python installers for Windows, Mac OS X and Linux operating systems. If you download an installer, it is of immense help because it comes with the Python interpreter, standard library, and standard modules. The standard library and built-in modules are specifically very important because they offer you several useful capabilities that will help you achieve your goal as an ethical hacker. Among the useful modules, you will get cryptographic services, Internet data handling, interaction with IP protocols, interoperability with the operating system, and many more. So go ahead, pick up any good beginner's book on Python, read the official documentation and know that it is a part of your learning schedule. Python is an extremely easy language to learn.

To create an ideal ethical hacker's environment, a few steps are extremely important. The steps include: installing Virtual Machine or Virtual Box (VB), having a basic knowledge about networking, and learning a useful programming language like Python. Let us first have a look at the basic networking knowledge.

Ethical Hacking and Networking

A basic knowledge about internetworking is extremely important if you want to learn ethical hacking. As you progress and want to go deeper, it is advisable to learn more about networking. Ethical hacking and internetworking are very closely associated. As you progress through this book you will find words like "packet," "switch," "router," "modem," "TCP/IP," "OSI," and many more.

The very first thing you need to know is: data travels through many layers. Ethical hackers try to understand these layers. Once they have understood the movement, they either want to track and block the data or they want to retrieve data.

In this chapter, we will very briefly see how internetworking models work. We will look into the different types of networking models. We will also learn about the devices that comprise a network.

What Does Network Mean?

A network is a collection of devices that are connected through media. One of the main characteristics of a network is: devices contain services and resources. Devices contain personal computers, switches, routers, and servers, among others. What do they do basically? They send data and get data either by switching or by routing. Actually, they connect users so that users ultimately get full data instead of getting it by pieces. So the basic services these devices provide include switching, routing, addressing, and data access.