Understanding Network Hacks

Bastian Ballmann

Understanding Network Hacks

Attack and Defense with Python 3

2nd Edition

Springer

Bastian Ballmann
Uster, Switzerland

ISBN 978-3-662-62156-1 ISBN 978-3-662-62157-8 (eBook)
https://doi.org/10.1007/978-3-662-62157-8

Responsible Editor: Martin Börger
This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

For data travelers, knowledge hungry, curious, network-loving lifeforms who like to explore and get to the bottom of thing.

Foreword

Doesn't this book explain how to break into a computer system? Isn't that illegal and a bad thing at all?

I would like to answer both questions with no (at least the second one). Knowledge is never illegal nor something bad, but the things you do with it.

You as an admin, programmer, IT manager or just an interested reader cannot protect yourself if you don't know the techniques of the attackers. You cannot test the effectiveness of your firewalls and intrusion detection systems or other security related software if you are not able to see your IT infrastructure through the eyes of an attacker. You cannot weigh up the danger to costs of possible security solutions if you don't know the risks of a successful attack. Therefore it is necessary to understand how attacks on computer networks really work.

The book presents a selection of possible attacks with short source code samples to demonstrate how easy and effectively and maybe undetected a network can be infiltrated. This way you can not only learn the real techniques, but present them to your manager or employer and help them in the decision if it would make sense to care a little bit more about IT security. At the end of the book you should be able to not only understand how attacks on computer networks really work, but also to modify the examples to your own environment and your own needs.

Sure, the book also tells those bad guys how to crack the net and write their own tools, but IT security is a sword with two sharp blades. Both sides feed themselves off the same pot of knowledge and it is an continuous battle, which the protecting side can never dream of winning if it censors itself or criminalizes their knowledge!

Introduction

Who should Read this Book?
This book addresses interested Python programmers who want to learn about network coding and to administrators, who want to actively check the security of their systems and networks. The content should also be useful for white, gray and black hat hackers, who prefer Python for coding, as well as for curious computer users, who want to get their hands on practical IT security and are interested in learning to see their network through the eyes of an attacker.

You neither need deep knowledge on how computer networks are build up nor in programming. You will get throught all the knowledge you need to understand the source codes of the book in Chaps. 2 and 3. Readers, who know how to program in Python and dream in OSI layers or packets headers can right away jump to Chap. 5 and start having fun at their device.

Of course a book like this needs a disclaimer and the author would be happy if all readers only play on systems they are allowed to do so and use the information of this book only for good and ethical actions otherwise you maybe breaking a law depending on the country your device is connected in.

The length of the book doesn't allow for in depth discussion of all topics. You will only get somewhat more than the basics. If you want to dig deeper you should afterwards get some special lecture in your special field of interest.

The Structure of the Book

The different hacks are grouped by network protocols and every chapters content is ordered by difficulty. You can read the book in the order you like except the both introduction chapters about networks (Chap. 2) and Python (Chap. 3).

The code samples are printed unshortened therefore you can just copy and use them without worrying about incremental changes or addons. All source codes presented in this book can also be found on Github at https://github.com/balle/python-network-hacks.

At the end of each chapter you will find a selection of tools also written in Python that attack the described protocol in a more detailed way.

Thanks to the basic knowledge learned in the chapter it shouldn't be too hard to read and understand the source code of the tools.

The Most Important Security Principles

The most important principles in building a secure network of the authors point of view are:

1. Security solutions should be simple. A firewall rule-set that no one understands, is a guarantee for security holes. Software that's complex has more bugs than simple code.
2. Less is more. More code, more systems, more services provide more possibilities of attack.
3. Security solutions should be Open Source. You can easier search for security problems if you have access to the source code. If the vendor disagrees to close an important security hole you or someone else can fix it and you don't have to wait for six or more months till the next patch day. Proprietary software can have build in backdoors sometimes called Law Interception Interface. Companies like Cisco (see RFC 3924), Skype (US-Patent-No 20110153809) and Microsoft (e.g. _NSAKEY http://en.wikipedia.org/wiki/NSAKEY) are only popular examples.
4. A firewall is a concept not a box that you plug in and you are safe.
5. Keep all your systems up to date! A system that's considered secure today can be unprotected a few hours later. Update all systems, also smart phones, printer and switches!
6. The weakest device defines the security of the complete system and that doesn't necessarily have to be a computer it can also be a human (read about social engineering).
7. There is no such thing as 100% secure. Even a computer that is switched off can be infiltrated by a good social engineer. The aim should be to build that much layers that the attacker falls over one tripwire and leaves traces and that the value he or she can gain from a successful infiltration is much lower than the effort to attack or that it exceeds the intruders skills.

Contents