Preface

"What is this Hacking School really about, you sick criminals?"

Are you shocked? Well, many irritated hacking pseudo-experts asked us such a question.

Congratulations. You hold this book in your hands - not everyone had such courage. This was the first and the most important step. Your first step towards mental revolution and the change of opinion about hacking. Let's start from the beginning.

We live in a society influenced by media. Every day, media bombards us with new visions of stereotypes and suggests how to perceive the world around us. To put it literally – media form our perception of the world. We used to divide people into fat and thin, clever and stupid, poor and rich, those 'backward pagans' and believers, and finally – into computer laymen and hackers.

Did you notice that?

Hackers are great people who live above the law. Every day, they invent new ways of breaking into computer systems and make shabby admins and other specialists angry. They take control over government networks and sometimes decide to deface some website or delete the content of some hard drive. Hackers break in everywhere. Banks, government institutions, CIA, FBI, NASA and KGB. They steal, eavesdrop, blackmail, force.

This is the picture of a hacker. Fortunately, it's the one created by media. Considering the definition above, this book should be entitled *'Anti-Hacking School'*, as it has nothing to do with the media nonsense. Let me explain you why.

Who are hackers?

There is one characteristic of a hacker that remained unchanged in the media definition. It is… outstanding **knowledge**.

Words 'hacker' and 'hacking' are often used in this book. For us hacking means discovering. Hackers represent knowledge. They have their own moral code. To discover – not to destroy. They work for the common good. The criminal that causes destruction and corresponds with the media definition is commonly called a 'cracker'.

Cracking is the opposite of hacking and the knowledge we want to give you in the Hacking School. If your intentions are different than the legal assumptions listed above, you can put this book back on the shelf.

But if you are ready to take another step towards adventure, broaden your perspective and start breathing the true air of bits and bytes, open yourself to new experiences and read further.

Hacking School Mission

Few years passed since the first issue of this book was printed and we still get new readers. Despite the public opinion and suggestions of the PR team, we still receive readers' interest due to the controversial title of the book and our promotional actions. Thanks to it, we have the chance to help you.

Would you take this book in your hands, if it was called *„Another technical manual on computer security"*? Probably not. We are successfull in meeting the interest of readers of different age and skills. We tell the truth about hacking and hacker's mission. We openly teach issues that are important to all of us. Without this knowledge, we would have no chance. We have to understand the threats coming from the cyber criminals to successfully protect ourselves.

Remember – we will show you many interesting hacking techniques but we trust your good intentions.

Our mission and the aim of this book is to make the reader aware of the existing threats and describe them in a comprehensible way. This is it.

Introduction

Dear reader!

We are delighted to be able to present this handbook to you. It is intended to provide you with a **solid foundation** in understanding computer and network security – a foundation understood by any self-respecting hacker.

With the help of this handbook you will proceed step-by-step through an **interactive course**, using both simple and advanced **techniques** that **hackers** employ every day. You will become acquainted with the methods of breaking through barriers and become familiar with knowledge that was until recently reserved to a small elite.

The method of passing knowledge that works

It is no coincidence that this publication is called a "handbook". As you will see, it is not just another dry, technical manual on the subject of computer systems security. What we have put together is an interactive educational system, one that will lead you through even the most difficult issues exploited by hackers.

Twenty out of the twenty one chapters in the handbook offer you the possibility to learn interactively, using a set of custom **video training materials** covering exactly the topics described in the handbook. Each of these films was created in a real-world environment and presents an authentic scenario that could be taken advantage of by a potential invader.

In addition, thanks to up-to-date commentaries and open access to the content presented within, you will have the opportunity to deepen your **understanding and practical knowledge** of each lesson. Each chapter may be accessed at any time. You may look at any part of the material whenever you like; it is entirely up to you.

Who is this book addressed to?

You don't have to worry if these are your first steps in the world of hacking. We created for you an independent **Training Operating System** that does not need to be installed. After two minutes your testing environment is ready to work. Easy, isn't it?

If you got this book within the entire set, you also received **interactive, 210 minutes long, Live Training Videos** (almost 4 hours of live training materials) and a specially prepared testing environment which will allow you to practice every lesson.

If you are an advanced user and you:

- Know the basic issues of the computer system and network security,
- Have access to a working testing environment,
- You know how to use it and you can compile new programs from source,
- You are able to cope with possible problems and prefer to solve them by yourself,
- You are guided by your own intuition and you go through all lessons according to your own vision of learning –

then you can successfully use this handbook to broaden your knowledge and conduct new interesting experiments. If it's not like this – don't worry, you will learn everything while reading the handbook.

What will I learn from this handbook?

On the next pages of this handbook you will find many issues regarding computer systems security.

The 21 chapters are a comprehensive overview of problems such as: **cracking passwords** of encrypted files; the **interception of information** across local area networks, whether sent as open text or using advanced encryption methods; **attacks carried out** on applications and data transmission

protocols; the **creation of exploits** and shellcode; the use of network scanners; **intrusion detection systems**; and security issues in instant messaging.

These examples are just a small sample of what is included in the handbook. For more details please look at the table of contents.

How to use the Hacking School Handbook?

The Hacking School Handbook is the heart of the whole educational set that we prepared for you. If you got the complete training set together with the Training Operating System and Live Training Videos, you should first get to know the content of the handbook.

To fully satisfy most senses used in the process of learning, we assumed what follows:

1. You get to know the issue while reading the chapter content in the handbook.
2. You watch the live training movie and analyze the actions taken by the hacker while reading the same lesson in the handbook. At the same time, you listen to the comments given by the lector in the movie.
3. Finally, you practice what you've learned in the Training Operating System environment.

You read, listen, watch and analyze the actions taken by the hacker in the movie. Then you practice everything what you have learned. If you think that you don't need additional comments and demonstrations to understand the current issue, you can skip the second point. It's up to you. The handbook is the fundament of the educational set and describes all issues in 90%.

Training Operating System and Live Training Videos

All source codes included in the handbook are also included in the Training Operating System in the /CD directory. While going through lesson X, you

have to enter the directory */CD/ChapterX*. The folders of given chapters contain subfolders: *Software* (packages with the software sources) and *Listings* (source codes of examples presented on the grey background).

For your comfort, all applications described and compiled in the handbook were included in the Training Operating System and do not have to be installed manually. However, if you want to compile any given application yourself, enter the */CD/ChapterX/Software* directory and do what is described in the handbook tips and training videos.

If you got this handbook without the additional elements (the Training Operating System and Live Training Videos), you can order them anytime – just send us an e-mail at contact@hackingschool.com and we'll provide you with the details.

Summary

Confucius, one of the greatest Chinese philosophers, said "***I listen and I forget. I see and I remember. I do and I understand.***" May this ancient Chinese wisdom be the main message of this book.