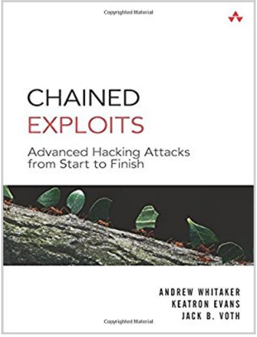

Chained Exploits: Advanced Hacking Attacks from Start to Finish

By Andrew Whitaker, Keatron Evans, Jack Voth

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth

The complete guide to today’s hard-to-defend chained attacks: performing them and preventing them

Nowadays, it’s rare for malicious hackers to rely on just one exploit or tool; instead, they use “chained” exploits that integrate multiple forms of attack to achieve their goals. Chained exploits are far more complex and far more difficult to defend. Few security or hacking books cover them well and most don’t cover them at all. Now there’s a book that brings together start-to-finish information about today’s most widespread chained exploits–both how to perform them and how to prevent them.

Chained Exploits demonstrates this advanced hacking attack technique through detailed examples that reflect real-world attack strategies, use today’s most common attack tools, and focus on actual high-value targets, including credit card and healthcare data. Relentlessly thorough and realistic, this book covers the full spectrum of attack avenues, from wireless networks to physical access and social engineering.

Writing for security, network, and other IT professionals, the authors take you through each attack, one step at a time, and then introduce today’s most effective countermeasures— both technical and human. Coverage includes:

- Constructing convincing new phishing attacks
- Discovering which sites other Web users are visiting
- Wreaking havoc on IT security via wireless networks
- Disrupting competitors’ Web sites
- Performing–and preventing–corporate espionage
- Destroying secure files
- Gaining access to private healthcare records
- Attacking the viewers of social networking pages
- Creating entirely new exploits
- and more

Andrew Whitaker, Director of Enterprise InfoSec and Networking for Training Camp, has been featured in The Wall Street Journal and BusinessWeek. He coauthored Penetration Testing and Network Defense. Andrew was a winner of EC Council’s Instructor of Excellence Award.

Keatron Evans is President and Chief Security Consultant of Blink Digital Security, LLC, a trainer for Training Camp, and winner of EC Council’s Instructor of Excellence Award.

Jack B. Voth specializes in penetration testing, vulnerability assessment, and perimeter security. He co-owns The Client Server, Inc., and teaches for Training Camp throughout the United States and abroad.

informit.com/aw
Cover photograph © Corbis /
Jupiter Images

$49.99 US
$59.99 CANADA

Chained Exploits: Advanced Hacking Attacks from Start to Finish

By Andrew Whitaker, Keatron Evans, Jack Voth

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth

The complete guide to today's hard-to-defend chained attacks: performing them and preventing them

Nowadays, it's rare for malicious hackers to rely on just one exploit or tool; instead, they use "chained" exploits that integrate multiple forms of attack to achieve their goals. Chained exploits are far more complex and far more difficult to defend. Few security or hacking books cover them well and most don't cover them at all. Now there's a book that brings together start-to-finish information about today's most widespread chained exploits–both how to perform them and how to prevent them.

Chained Exploits demonstrates this advanced hacking attack technique through detailed examples that reflect real-world attack strategies, use today's most common attack tools, and focus on actual high-value targets, including credit card and healthcare data. Relentlessly thorough and realistic, this book covers the full spectrum of attack avenues, from wireless networks to physical access and social engineering.

Writing for security, network, and other IT professionals, the authors take you through each attack, one step at a time, and then introduce today's most effective countermeasures— both technical and human. Coverage includes:

- Constructing convincing new phishing attacks
- Discovering which sites other Web users are visiting
- Wreaking havoc on IT security via wireless networks
- Disrupting competitors' Web sites
- Performing–and preventing–corporate espionage
- Destroying secure files
- Gaining access to private healthcare records
- Attacking the viewers of social networking pages
- Creating entirely new exploits
- and more

Andrew Whitaker, Director of Enterprise InfoSec and Networking for Training Camp, has been featured in The Wall Street Journal and BusinessWeek. He coauthored Penetration Testing and Network Defense. Andrew was a winner of EC Council's Instructor of Excellence Award.

Keatron Evans is President and Chief Security Consultant of Blink Digital Security, LLC, a trainer for Training Camp, and winner of EC Council's Instructor of Excellence Award.

Jack B. Voth specializes in penetration testing, vulnerability assessment, and perimeter security. He co-owns The Client Server, Inc., and teaches for Training Camp throughout the United States and abroad.

informit.com/aw

Cover photograph © Corbis /
Jupiter Images

$49.99 US
$59.99 CANADA

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth Bibliography

- Sales Rank: #889273 in Books
- Published on: 2009-03-09
- Released on: 2009-02-27
- Original language: English
- Number of items: 1
- Dimensions: 9.20" h x .70" w x 7.00" l, 1.09 pounds
- Binding: Paperback
- 312 pages

Introduction

Whenever we tell people about the contents of this book, we always get the same response: “Isn’t that illegal?” Yes, we tell them. Most of what this book covers is completely illegal if you re-create the scenarios and perform them outside of a lab environment. This leads to the question of why we would even want to create a book like this.

The answer is quite simple. This book is necessary in the marketplace to educate others about chained exploits. Throughout our careers we have helped secure hundreds of organizations. The biggest weakness we saw was not in engineering a new security solution, but in education. People are just not aware of how attacks really occur. They need to be educated in how the sophisticated attacks happen so that they can know how to effectively protect against them.

All the authors of this book have experience in both penetration testing (hacking into organizations with authorization to assess their weakness) as well as teaching security and ethical hacking courses for Training Camp (http://www.trainingcamp.com). Many of the chapters in this book come from attacks we have successfully performed in real-world penetration tests. We want to share these so that you know how to stop malicious attacks. We all agree that it is through training that we make the biggest impact, and this book serves as an extension to our passion for security awareness training.

What Is a Chained Exploit?

There are several excellent books in the market on information security. What has been lacking, however, is a book that covers chained exploits and effective countermeasures. A chained exploit is an attack that involves multiple exploits or attacks. Typically a hacker will use not just one method, but several, to get to his or her target.

Take this scenario as an example. You get a call at 2 a.m. from a frantic coworker, saying your Web site has been breached. You jump out of bed, throw on a baseball cap and some clothes, and rush down to your workplace. When you get there, you find your manager and coworkers frenzied about what to do. You look at the Web server and go through the logs. Nothing sticks out at you. You go to the firewall and review its logs. You do not see any suspicious traffic heading for your Web server. What do you do?

We hope you said, “Step back, and look at the bigger picture.” Look around your infrastructure. You might have dedicated logging machines, load-balancing devices, switches, routers, backup devices, VPN (virtual private network) devices, hubs, database servers, application servers, Web servers, firewalls, encryption devices, storage devices, intruder detection devices, and much more. Within each of these devices and servers runs software. Each piece of software is a possible point of entry.

In this scenario the attacker might not have directly attacked the Web server from the outside. He or she might have first compromised a router. From there, the attacker might reconfigure the router to get access to a backup server that manages all backups for your datacenter. Next the attacker might use a buffer overflow exploit against your backup software to get administrator access to the backup server. The attacker might launch an attack to confuse the intrusion detection system so that the real attack goes unnoticed. Then the attacker might launch an attack from the backup server to a server that stores all your log files. The attacker might erase all log files to cover his or her tracks, and then launch an attack from that server to your Web server. We think you get the point: Attacks are seldom simple. They often involve many separate attacks chained together to form one large attack. Your job as a security professional is to be constantly aware of the big picture, and to consider everything when someone attacks your system.

A skilled hacker acts much like the ants on the cover of this book. If you notice on the cover, the ants are in a line, each separate, but part of a chain. Each ant also takes something for its own use, like a hacker stealing information. Ants also tend to do most of their work without anyone seeing them, just as skilled hackers do their work without observation. Use this book as your pesticide; learn where the hackers are hiding so that you can eliminate them and stop them from gaining access to your organization.

Format of the Book

This book makes use of a fictional character named Phoenix. You do not need to read the chapters in any particular order, so if you want to jump into a topic of interest right away, go for it. Each chapter begins with a “Setting the Stage” section where we explain the scenario that is the basis behind Phoenix’s motivation for attack. You’ll learn how common greed or the desire for revenge can lead to sophisticated attacks with serious consequences.

Each chapter continues with a section titled “The Chained Exploit,” which is a detailed, step-by-step approach used by our fictitious character to launch his attack. As you read through this section, you will learn that an attack is more than just using one software tool to gain access to a computer. Sometimes attacks originate from within an organization, whereas other times attacks begin from outside the organization. You will even learn about compromising physical security and social engineering as means to achieving Phoenix’s goal.

Each chapter concludes with a “Countermeasures” section filled with information that you can use to prevent the chained exploit discussed in the chapter. You should compare this information with your own security policies and procedures to determine whether your organization can or should deploy these countermeasures.

Note - Many of the organizations and Web sites mentioned in the scenario portions of this book are fictitious and are for illustrative purposes only. For example, in Chapter 2, “Discover What Your Boss Is Looking At,” the http://www.certificationpractice.com site Phoenix copies for his phishing site does not really exist, although many like it do.

Additional Resources

There were many things we wanted to include in this book but could not due to time restraints. You can find more information about chained exploits by visiting http://www.chainedexploits.com. That Web site contains additional information about chained exploits and any errata for this book.

Disclaimer

The attacks in this book are illegal if performed outside a lab environment. All the examples in this book are from the authors’ experience performing authorized penetration tests against organizations. Then the authors re-created the examples in a lab environment to ensure accuracy. At no point should you attempt to re-create any of these attacks described in this book. Should you want to use the techniques to assess the security of your organization, be sure to first obtain written authorization from key stakeholders and appropriate managers before you perform any tests.

Read Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth for online ebook

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth books to read online.

Online Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth ebook PDF download

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth Doc

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth Mobipocket

Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth EPub

C6KMYW8DAPJ: Chained Exploits: Advanced Hacking Attacks from Start to Finish By Andrew Whitaker, Keatron Evans, Jack Voth