COMPUTER SECURITY FUNDAMENTALS

THIRD EDITION

CHUCK EASTTOM

Computer Security Fundamentals

Third Edition

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Computer Security Fundamentals, Third Edition

ISBN-13: 978-0-7897-5746-3
ISBN-10: 0-7897-5746-X

Library of Congress control number: 2016940227

Printed in the United States of America

First Printing: May 2016

Executive Editor
Brett Bartow

Acquisitions Editor
Betsy Brown

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Gill Editorial Services

Indexer
Brad Herriman

Proofreader
Paula Lowell

Technical Editor
Dr. Louay Karadsheh

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Mary Sudul

Contents at a Glance

Table of Contents

About the Author

Chuck Easttom is a computer security and forensics expert. He has authored 20 books, including several on computer security, forensics, and cryptography. He holds 6 patents and 40 computer certifications, including many security and forensics certifications. He has conducted training for law enforcement, federal agencies, and friendly foreign governments. He frequently works as an expert witness in computer-related cases. He is also a frequent speaker on computer security topics at a variety of security-related conferences. You can visit his website at www.chuckeasttom.com.

About the Technical Reviewer

Dr. Louay Karadsheh has a Doctorate of Management in information technology from Lawrence Technological University, Southfield, Michigan. His research interest includes cloud computing, information assurance, knowledge management, and risk management. Dr. Karadsheh has published 11 articles in refereed journals and international conference proceedings and has extensive knowledge in operating system, networking, and security. Dr. Karadsheh has provided technical edits/reviews for several major publishing companies, including Pearson and Cengage Learning. He holds CISSP, CEH, CASP, CCSK, CCE, Security+, VCA-C, VCA-DCV, SCNP, Network+, and Mobility+ certifications.

Dedication

This book is dedicated to my wife, Teresa,
who has helped me become who I am.

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication from many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project.

Specifically, I would like to say thanks to Betsy Brown for overseeing the project and keeping things moving.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *Computer Security Fundamentals* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789757463 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

It has been more than 10 years since the publication of the original edition of this book. A great deal has happened in the world of computer security since that time. This edition is updated to include newer information, updated issues, and revised content.

The real question is: Who is this book for? This book is a guide for any computer-savvy person. That means system administrators who are not security experts or anyone who has a working knowledge of computers and wishes to know more about cyber crime and terrorism could find this book useful. However, the core audience will be students who wish to take a first course in security but may not have a thorough background in computer networks. The book is in textbook format, making it ideal for introductory computer security courses that have no specific prerequisites. That lack of prerequisites means that people outside the normal computer science and computer information systems departments could also avail themselves of a course based on this book. This might be of particular interest to law enforcement officers, criminal justice majors, and even business majors with an interest in computer security.

As was previously mentioned, this book is intended as an introductory computer security book. In addition to the numerous end notes, the appendixes will guide you to a plethora of additional resources. There are also review questions and practice exercises with every chapter. Appendix C contains the answers to the multiple choice questions for your review. Exercises and projects don't have a single answer. They are intended to encourage the reader to explore, so answers will vary.

This book is not a cookbook for hackers. You will see exactly how hackers target a system and get information about it. You will also see step-by-step instructions on how to use some password-cracking utilities and some network-scanning utilities. You will also be given a reasonably in-depth explanation of various hacking attacks. However, you won't see a specific step-by-step recipe for executing an attack.

This book assumes that you are a competent computer user. That means you have used a computer at work and at home, are comfortable with email and web browsers, and know what words like RAM and USB mean. For instructors considering this as a textbook, that means students will have had some basic understanding of PCs but need not have had formal computer courses. For this reason, there is a chapter on basic networking concepts to get you up to speed. For readers with more knowledge, such as system administrators, you will find some chapters of more use to you than others. Feel free to simply skim any chapter that you feel is too elementary for you.

Chapter 1

Introduction to Computer Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Identify the top threats to a network: security breaches, denial of service attacks, and malware
- Assess the likelihood of an attack on your network
- Define key terms such as *cracker*, *penetration tester*, *firewall*, and *authentication*
- Compare and contrast perimeter and layered approaches to network security
- Use online resources to secure your network

Introduction

Since the first edition of this book, the prevalence of online transactions has increased dramatically. In 2004 we had e-commerce via websites; in 2016 we have smart phone apps, the Internet of Things, as well as an expanded use of e-commerce websites. Internet traffic is far more than just humorous YouTube videos or Facebook updates about our vacations. Now it is the heart and soul of commerce, both domestic and international. Internet communication even plays a central role in military operations and diplomatic relations. In addition to smart phones, we now have smart watches and even vehicles that have Wi-Fi hotspots and smart technology. Our lives are inextricably intertwined with the online world. We file our taxes online, shop for a home online, book our next vacation online, and even look for a date online.

Because so much of our business is transacted online, a great deal of personal information is stored in computers. Medical records, tax records, school records, and more are all stored in computer databases. This leads to some very important questions:

1. How is information safeguarded?
2. What are the vulnerabilities to these systems?
3. What steps are taken to ensure that these systems and data are safe?
4. Who can access my information?

FYI: Where Is the Internet Going?

Obviously the Internet has expanded, as previously mentioned. We now have smart phones, smart watches, even smart cars. We have the Internet of things (IoT) which involves devices communicating on the Internet. What do you think the next 10 years will bring?

Unfortunately, not only has technology and Internet access expanded since the original publication of this book, but so have the dangers. How serious is the problem? According to a 2014 article in *SC Magazine*,[1] "Cyber-crime and economic espionage cost the global economy more than $445 billion annually, which a report from the Center for Strategic and International Studies, says puts cyber-crime on par with the economic impact of global drug trafficking."

Another study[2] looked at specific companies and the cost of cybercrime in 2013. That study reported, "We found that the average annualized cost of cyber-crime for 60 organizations in our study is $11.6 million per year, with a range of $1.3 million to $58 million. In 2012, the average annualized cost was $8.9 million. This represents an increase in cost of 26 percent or $2.6 million from the results of our cyber cost study published last year."

The situation is not improving, either. According to a Pricewaterhouse Coopers study, in 2015 38% more security incidents were detected than in 2014. The same study showed a 56% increase in theft of intellectual property.

In spite of daily horror stories, however, many people (including some law enforcement professionals and trained computer professionals) lack an adequate understanding about the reality of these threats. Clearly the media will focus attention on the most dramatic computer security breaches, not necessarily giving an accurate picture of the most plausible threat scenarios. It is not uncommon to encounter the occasional system administrator whose knowledge of computer security is inadequate.

This chapter outlines current dangers, describes the most common types of attacks on your personal computer and network, teaches you how to speak the lingo of both hackers and security professionals, and outlines the broad strokes of what it takes to secure your computer and your network.

In this book, you will learn how to secure both individual computers and entire networks. You will also find out how to secure data transmission, and you will complete an exercise to find out about your region's laws regarding computer security. Perhaps the most crucial discussion in this chapter is what

1. http://www.scmagazine.com/cyber-crime-costs-445-billion-globally-gdps-take-hit/article/354844/
2. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

attacks are commonly attempted and how they are perpetrated. In this first chapter we set the stage for the rest of the book by outlining what exactly the dangers are and introducing you to the terminology used by both network security professionals and hackers. All of these topics are explored more fully in subsequent chapters.

How Seriously Should You Take Threats to Network Security?

The first step in understanding computer and network security is to formulate a realistic assessment of the threats to those systems. You will need a clear picture of the dangers in order to adequately prepare a defense. There seem to be two extreme attitudes regarding computer security. The first group assumes there is no real threat. Subscribers to this belief feel that there is little real danger to computer systems and that much of the negative news is simply unwarranted panic. They often believe taking only minimal security precautions should ensure the safety of their systems. The prevailing sentiment is, if our organization has not been attacked so far, we must be secure. If decision makers subscribe to this point of view, they tend to push a reactive approach to security. They will wait to address security issues until an incident occurs—the proverbial "closing the barn door after the horse has already gotten out." If you are fortunate, the incident will have only minor impact on your organization and will serve as a much-needed wakeup call. If you are unfortunate, then your organization may face serious and possible catastrophic consequences. One major goal of this book is to encourage a proactive approach to security.

People who subscribe to the opposite viewpoint overestimate the dangers. They tend to assume that talented, numerous hackers are an imminent threat to their system. They may believe that any teenager with a laptop can traverse highly secure systems at will. Such a worldview makes excellent movie plots, but it is simply unrealistic. The reality is that many people who call themselves hackers are less knowledgeable than they think they are. These people have a low probability of being able to compromise any system that has implemented even moderate security precautions.

This does not mean that skillful hackers do not exist, of course. However, they must balance the costs (financial, time) against the rewards (ideological, monetary). "Good" hackers tend to target systems that yield the highest rewards. If a hacker doesn't perceive your system as beneficial to these goals, he is less likely to expend the resources to compromise your system. It is also important to understand that real intrusions into a network take time and effort. Hacking is not the dramatic process you see in movies. I often teach courses in hacking and penetration testing, and students are usually surprised to find that the process is actually a bit tedious and requires patience.

Both extremes of attitudes regarding the dangers to computer systems are inaccurate. It is certainly true that there are people who have the understanding of computer systems and the skills to compromise the security of many, if not most, systems. A number of people who call themselves hackers, though, are not as skilled as they claim to be. They have ascertained a few buzzwords from the Internet and may be convinced of their own digital supremacy, but they are not able to effect any real compromises to even a moderately secure system.

The truly talented hacker is no more common than the truly talented concert pianist. Consider how many people take piano lessons at some point in their lives. Now consider how many of those ever truly become virtuosos. The same is true of computer hackers. Keep in mind that even those who do possess the requisite skills need to be motivated to expend the time and effort to compromise your system.

A better way to assess the threat level to your system is to weigh the attractiveness of your system to potential intruders against the security measures in place.

Keep in mind, too, that the greatest external threat to any system is not hackers, but malware and denial of service (DoS) attacks. Malware includes viruses, worms, Trojan horses, and logic bombs. And beyond the external attacks, there is the issue of internal problems due to malfeasance or simple ignorance.

Security audits always begin with a risk assessment, and that is what we are describing here. First you need to identify your assets. Clearly, the actual computers, routers, switches and other devices that make up your network are assets. But it is more likely that your most important assets lie in the information on your network. Identifying assets begins with evaluating the information your network stores and its value. Does your network contain personal information for bank accounts? Perhaps medical information, health care records? In other cases your network might contain intellectual property, trade secrets, or even classified data.

Once you have identified the assets, you need to take inventory of the threats to your assets. Certainly any threat is possible, but some are more likely than others. This is very much like what one does when selecting home insurance. If you live in a flood plain, then flood insurance is critical. If you live at a high altitude in a desert, it may be less critical. We do the same thing with our data. If you are working for a defense contractor, then foreign state-sponsored hackers are a significant threat. However, if you are the network administrator for a school district, then your greatest threat involves juveniles attempting to breach the network. It is always important to realize what the threats are for your network.

Now that you have identified your assets and inventoried the threats, you need to find out what vulnerabilities your system has. Every system has vulnerabilities. Identifying your network's specific vulnerabilities is a major part of risk assessment.

The knowledge of your assets, threats, and vulnerabilities will give you the information needed to decide what security measures are appropriate for your network. You will always have budget constraints, so you will need to make wise decisions on selecting security controls. Using good risk assessment is how you make wise security decisions.

Note

There are a number of industry certifications that emphasize risk assessment. The Certified Information System's Security Professional (CISSP) puts significant emphasis on this issue. The Certified Information Systems Auditor (CISA) places even more focus on risk assessment. One or more appropriate industry certifications can enhance your skillset and make you more marketable as a security professional. There are many other certifications including the CompTIA Certified Advanced Security Practitioner (CASP) and Security+ certifications.

Identifying Types of Threats

As was discussed in the last section, identifying your threats is a key part of risk assessment. Some threats are common to all networks; others are more likely with specific types of networks. Various sources have divided threats into different categories based on specific criteria. In this section we will examine threats that have been divided into categories based on the nature of the attack. Since the last edition of this book I have separated out one of the security breach subcategories into its own category: insider threats. Most attacks can be categorized as one of seven broad classes:

- **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.
- **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server…all the things you probably associate with the term *hacking*.
- **DoS attacks:** These are designed to prevent legitimate access to your system. And, as you will see in later chapters, this includes distributed denial of service (DDoS).
- **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session hijacking:** These attacks are rather advanced and involve an attacker attempting to take over a session.
- **Insider threats:** These are breaches based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

There are other attacks, such as social engineering. The forgoing list is just an attempt to provide a broad categorization of attack types. This section offers a broad description of each type of attack. Later chapters go into greater detail with each specific attack, how it is accomplished, and how to avoid it.

Malware

Malware is a generic term for software that has a malicious purpose. This section discusses four types of malware: viruses, Trojan horses, spyware, and logic bombs. Trojan horses and viruses are the most widely encountered. One could also include rootkits, but these usually spread as viruses and are regarded as simply a specific type of virus.

According to Symantec (makers of Norton antivirus and other software products), a *virus* is "a small program that replicates and hides itself inside other programs, usually without your knowledge"

(Symantec, 2003). While this definition is a bit old, it still applies. The key characteristic of a computer virus is that it self-replicates. A computer virus is similar to a biological virus; both are designed to replicate and spread. The most common method for spreading a virus is using the victim's email account to spread the virus to everyone in his address book. Some viruses don't actually harm the system itself, but *all* of them cause network slowdowns due to the heavy network traffic caused by the virus replication.

The *Trojan horse* gets its name from an ancient tale. The city of Troy was besieged for an extended period of time. The attackers could not gain entrance, so they constructed a huge wooden horse and one night left it in front of the gates of Troy. The next morning the residents of Troy saw the horse and assumed it to be a gift, so they rolled the wooden horse into the city. Unbeknownst to them, several soldiers where hidden inside the horse. That evening the soldiers left the horse, opened the city gates, and let their fellow attackers into the city. An electronic Trojan horse works the same way, appearing to be benign software but secretly downloading a virus or some other type of malware onto your computer from within.

Another category of malware currently on the rise is *spyware*. Spyware is simply software that literally spies on what you do on your computer. Spyware can be as simple as a *cookie*—a text file that your browser creates and stores on your hard drive—that a website you have visited downloads to your machine and uses to recognize you when you return to the site. However, that flat file can then be read by the website or by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked. Spyware may also consist of software that takes periodic screenshots of the activity on your computer and sends those to the attacker.

Another form of spyware, called a *key logger*, records all of your keystrokes. Some key loggers also take periodic screenshots of your computer. Data is then either stored for later retrieval by the person who installed the key logger or is sent immediately back via email. We will discuss specific types of key loggers later in this book.

A *logic bomb* is software that lays dormant until some specific condition is met. That condition is usually a date and time. When the condition is met, the software does some malicious act such as delete files, alter system configuration, or perhaps release a virus. In Chapter 5, "Malware," we will examine logic bombs and other types of malware in detail.

Compromising System Security

Next we will look at attacks that breach your system's security. This activity is what is commonly referred to as *hacking*, though that is not the term hackers themselves use. We will delve into appropriate terminology in just a few pages; however, it should be noted at this point that *cracking* is the appropriate word for intruding into a system without permission, usually with malevolent intent. Any attack that is designed to breach your security, either via some operating system flaw or any other means, can be classified as cracking.

Essentially any technique to bypass security, crack passwords, breach Wi-Fi, or in any way actually gain access to the target network fits into this category. That makes this a very broad category indeed.

However, not all breaches involve technical exploits. In fact, some of the most successful breaches are entirely nontechnical. *Social engineering* is a technique for breaching a system's security by exploiting human nature rather than technology. This was the path that the famous hacker Kevin Mitnick most often used. Social engineering uses standard con techniques to get users to give up the information needed to gain access to a target system. The way this method works is rather simple: The perpetrator gets preliminary information about a target organization and leverages it to obtain additional information from the system's users.

Following is an example of social engineering in action. Armed with the name of a system administrator, you might call someone in the business's accounting department and claim to be one of the company's technical support personnel. Mentioning the system administrator's name would help validate that claim, allowing you to ask questions in an attempt to ascertain more details about the system's specifications. A savvy intruder might even get the accounting person to say a username and password. As you can see, this method is based on how well the prospective intruder can manipulate people and actually has little to do with computer skills.

The growing popularity of wireless networks gave rise to new kinds of attacks. One such activity is *war-driving*. This type of attack is an offshoot of *war-dialing*. With war-dialing, a hacker sets up a computer to call phone numbers in sequence until another computer answers to try to gain entry to its system. War-driving is much the same concept, applied to locating vulnerable wireless networks. In this scenario, the hacker simply drives around trying to locate wireless networks. Many people forget that their wireless network signal often extends as much as 100 feet (thus, past walls). At the 2004 DefCon convention for hackers, there was a war-driving contest where contestants drove around the city trying to locate as many vulnerable wireless networks as they could (BlackBeetle, 2004). These sorts of contests are now common at various hacking conventions.

Recent technological innovations have introduced new variations of war driving/dialing. Now we have war flying. The attacker uses a small private drone equipped with Wi-Fi sniffing and cracking software, flies the drone in the area of interest, and attempts to gain access to wireless networks.

Of course, Wi-Fi hacking is only one sort of breach. Password cracking tools are now commonly available on the Internet. We will examine some of these later in this book. There are also exploits of software vulnerabilities that allow one to gain access to the target computer.

DoS Attacks

In a DoS, the attacker does not actually access the system. Rather, this person simply blocks access from legitimate users (CERT, 2003). One common way to prevent legitimate service is to flood the targeted system with so many false connection requests that the system cannot respond to legitimate requests. DoS is a very common attack because it is so easy.

In recent years there has been a proliferation of DoS tools available on the Internet. One of the most common such tools is the Low Orbit Ion Cannon (LOIC). Because these tools can be downloaded for free from the Internet, anyone can execute a DoS attack, even without technical skill.

We also have variations, such as the DDoS attack. This uses multiple machines to attack the target. Given that many modern websites are hosted in network clusters or even in clouds, it is very difficult for a single attacking machine to generate enough traffic to take down a web server. But a network of hundreds or even thousands of computers certainly can. We will explore DoS and DDoS attacks in more detail in Chapter 4, "Denial of Service Attacks."

Web Attacks

By their nature, web servers have to allow communications. Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands. The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

SQL Injection

SQL injection is still quite common, though it has been known for many years. Unfortunately, not enough web developers take the appropriate steps to remediate the vulnerabilities that make this attack possible. Given the prevalence of this attack, it warrants a bit more detailed description.

Consider one of the simplest forms of SQL injection, used to bypass login screens. The website was developed in some web programming language, such as PHP or ASP.NET. The database is most likely a basic relational database such as Oracle, SQL Server, MySQL, or PostGres. SQL is used to communicate with the database, so we need to put SQL statements into the web page that was written into some programming language. That will allow us to query the database and see if the username and password are valid.

SQL is relatively easy to understand; in fact, it looks a lot like English. There are commands like `SELECT` to get data, `INSERT` to put data in, and `UPDATE` to change data. In order to log in to a website, the web page has to query a database table to see if that username and password are correct. The general structure of SQL is like this:

```
select column1, column2 from tablename
```

or

```
select * from tablename;
Conditions:
select columns from tablename where condition;
```

For example:

```
SELECT * FROM tblUsers WHERE USERNAME = 'jsmith'
```