INTRODUCTION

This book is an introduction to cybersecurity, written to help system and network administrators and owners understand the fundamentals of securing a network. Your personal cybersecurity is critical in protecting yourself from fraud and other harmful events attempted by adversaries. It's easy to tell yourself that you can't be a target, that you have nothing an adversary would want to use or exploit. However, your personal identifiable information (PII), protected health information (PHI), intellectual property, and government information and identification all have value. Failing to protect those things can lead to consequences such as identify theft, which can have a serious impact on your life.

For our purposes, a small network consists of 100 or fewer *endpoints*. An endpoint, or *host*, is any system or device that connects to or is part of a network, such as a desktop or laptop computer or a mobile device like a phone or tablet. Larger networks, approaching the size of an enterprise network, use similar tools and techniques that are covered in this book to provide security to their users and systems, just on a much larger scale and often at a much higher cost.

The drawback to securing small networks is that you have to maintain and administer everything yourself, with limited support and likely a

limited budget. Securing your network will require constant care, and we'll cover some ways that you can do this cheaply when the need arises. Ultimately, the goal of this book is to arm you with the tools and knowledge to secure your network with whatever resources you have available, in terms of both time and money.

How to Use This Book: What to Expect

This book is written so that if you follow it logically from chapter to chapter, you'll progress through several levels of security maturity, ending with a network that has a *defense-in-depth* architecture. Defense-in-depth is an approach to cybersecurity where several defensive solutions are layered to protect valuable data and information. **Chapters 1 to 4** cover how to design and architect your network to better enable your defenses and network monitoring capabilities. Then, **Chapters 5 to 8** discuss low-cost, high-impact passive defense strategies to prevent adversaries from gaining access to your network or endpoints. Finally, **Chapters 9 to 11** focus on the value of regular backups and active defenses, whereby you receive and respond to alerts to suspicious or malicious activity in your network, enabling cyber incident response.

Most chapters contain stand-alone projects. You can choose to complete each project in order, or you can pick and choose which projects you want to complete. However, the concepts covered in earlier chapters on network architecture provide the best return on investment, in terms of both time and money, and require less ongoing support and maintenance. The later chapters that cover active defenses require constant monitoring and are made more efficient with the completion of earlier projects. In some cases, working through the projects in earlier chapters also provides baseline knowledge that may be useful in later projects, such as familiarity with the command line. Essentially, you should complete each chapter in whichever order makes the most sense for you and your environment; for example, if you already have host and network firewalls in place, you can probably skip **Chapter 3**.

I recommend starting with **Chapter 1** before setting off on your own adventure. It covers two fundamental topics: setting up the servers you'll use throughout the book and creating a network map and asset list. Before you can secure your network, you need to understand its *topology*: which hosts are connected to it and how they connect to each other. Mapping the topology will help you keep track of your devices and recognize unusual activity on the network. It's expected that the vast majority of readers will implement the projects contained in this book as virtual machines (VMs). *Virtual machines* (which are also endpoints!) let you run multiple computers using one physical computer. Using VMs is a cheaper and easier way to achieve the same results with fewer hardware requirements. (I'll describe the remaining hardware recommendations in the section "**Recommended Hardware**.")

Recommended (But Not Required) Knowledge

In this book, you'll learn the fundamentals of cybersecurity as it relates to securing small networks. The book will guide you through all of the necessary steps to complete each chapter and project at a very low level. Having previous experience working with virtual machines, using the command line, and generally managing or administering a network of any size will prove beneficial. Having said that, you should be able to follow along regardless of experience, as you'll learn the necessary skills as you progress.

Recommended Hardware

Some of the projects in this book may require hardware or a device or system that you may not currently have on hand. Wherever possible, alternatives will be provided to purchasing new hardware, but in some cases, you might find the best or only way forward is to buy something new. What follows is a list of the hardware used in each chapter.

Virtual Machine Host System

- You can use a computer you already have to run your virtual machines, so long as that physical computer has enough memory (RAM) and processor (CPU) resources. As a general rule, you'll need 2GB of memory and one CPU core for each VM you plan to run, plus at least 4GB of memory and one CPU core for the host operating system. Therefore, to complete every chapter of this book, you should plan to use a physical system with at least 16GB of RAM and eight CPU cores.
- Most modern systems come with specifications of this level, and you can also use network attached storage (NAS) or another system capable of running virtual machines, or a small computing unit such as an Intel NUC, in the same way. A NAS is a device connected to your network that allows storage and retrieval of data from a central location and in most cases will offer additional network services and capabilities, like the ability to host virtual machines. If you have spare resources on your computer, start there. You can always move your virtual machines to a new system if they outgrow their original host and its hardware.

Firewall

- In **Chapter 3**, you'll be led through the installation and configuration of a pfSense firewall. This firewall can be purchased cheaply, and it will go a long way in increasing the security of any network very quickly and with minimal effort. The recommended device is the Netgate SG-3100 as it's cost-effective and easy to set up and maintain. It is possible to build your own, but the Netgate will likely be more secure and have a better cost.

NOTE *Netgate's pfSense SG-3100 has been discontinued. We recommend using the Netgate 2100 or 4100 instead. The configuration options will still be equivalent to what is described in the book.*

Wireless Router

- If you plan to use wireless in your small network (it's expected that the majority of your devices will be wirelessly connected), you'll need a wireless router or access point. We'll use the ASUS RT-AC5300 for most of the relevant examples in this book. This router is a mid-range device in terms of price and features. It provides enterprise-grade functionality without the premium price tag.

NOTE *The ASUS RT-AC5300 has been discontinued. For best value, we recommend using the ASUS RT-AX55 or ASUS RT-AC86U, but any AC/AX series ASUS router should have the same interface and configuration options.*

Managed Switch

- A *managed switch* is a device that can be configured to monitor and control network traffic. This is another relatively low-cost device that will provide you with very useful capabilities, like the ability to keep vulnerable and valuable devices separate. We'll mostly be discussing and using the Netgear GS308E.

Network TAP

- A *network tap* is a monitoring device that mirrors traffic passing between two points on a network, allowing you to collect network traffic as it travels between devices as well as networks. You can analyze captured traffic to identify suspicious or malicious behavior and then tailor your defenses to prevent or alert on that activity, providing the best chance to prevent cybersecurity incidents. Dualcomm offers several TAPs with varying capabilities, capacities, and price points. For most small networks, the ETAP-2003 will be sufficient; this is the device we'll focus on.

Alternatives

- While the step-by-step instructions will be tailored to these recommended devices, the processes are generalized enough that you should be able to follow them with any other similar devices. Alternatives to all the devices recommended in this introduction are devices available from Ubiquiti. While Ubiquiti devices will be more expensive, they provide greater functionality and ease of administration, and they offer commercial support.

Summary

If you want to begin your security journey in the most cost-effective way possible, complete **Chapters 1 to 4** on creating a defensible network architecture. If your interests lie more in the network monitoring, detection, and incident prevention domains, dive into **Chapters 5 to 8** to learn high-impact defense strategies for mitigating cyber vulnerabilities and preventing adversary access to your endpoints. If your network and defense capabilities are somewhat mature already, investigate **Chapters 9 to 11** for more active strategies to protect your network, endpoints, and users from adversaries that might be targeting your personal information or business data.