CYBERSECURITY
BLUE TEAM TOOLKIT

NADEAN H. TANNER

WILEY

Cybersecurity Blue Team Toolkit

Cybersecurity Blue Team Toolkit

Nadean H. Tanner

WILEY

Cybersecurity Blue Team Toolkit

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-119-55293-2
ISBN: 978-1-119-55295-6 (ebk)
ISBN: 978-1-119-55294-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019933354

To my wonderful husband Kenneth, who believes I can do anything.
Without your support, this would not have happened.

To my brown eyes—Shelby, if a film is made, I promise you the lead role.

To my blue eyes—Gavin, thank you for all your electronical advice.

I love you—infinity times googleplex.

About the Author

When my 7-year-old introduced me to his second-grade class, he put it best: "My mom teaches the good guys how to keep the bad guys out of their computers. She has a blue light saber."

I have been in the technology industry for more than 20 years in a variety of positions from marketing to training to web development to hardware. I have worked in academia as an IT director of a private elementary/middle school and as a technology instructor teaching post-graduate classes at Louisiana State University. I have trained and consulted in the corporate world for Fortune 50 companies and have hands-on experience working and training the U.S. Department of Defense, focusing on advanced cybersecurity and certifications. Currently, I am Lead Education Technical Specialist at Rapid7, managing the curriculum and teaching classes in Nexpose, InsightVM, Metasploit, Ruby, SQL, and API.

I love what I do—as an author, a trainer, and an engineer—making the world safer one domain at a time.

Current certifications:

A+
Network+
Security+
CASP
Server+
CIOS
CNIP
CSIS
CISSP
MCSA
MCITP
MCTS
MCP
AVM
NCP
MPCS
IICS
IVMCS
ITILv3

About the Technical Editor

Emily Adams-Vandewater (SSCP, Security+, Cloud+, CSCP, MCP) is a technical strategies and security manager at Flexible Business Systems, an MSP located on Long Island, New York, where she focuses on network security and vulnerability management, backup and data recovery, endpoint protection, and incident response. She holds certifications and expertise in malware and cyber intrusion analysis, detection, and forensics. Emily is an active and passionate member of a variety of Women in Technology groups and shares her knowledge by volunteering as a cybersecurity subject-matter expert for ICS2 exam development and a variety of cybersecurity conferences. When Emily is not working, she spends her time learning new security tools and technologies to satisfy her drive to learn and unrelenting curiosity of the unknown.

Credits

Associate Publisher
Jim Minatel

Editorial Manager
Pete Gaughan

Production Manager
Katie Wisor

Project Editor
Kathryn Duggan

Production Editor
Barath Kumar Rajasekaran

Technical Editor
Emily Adams-Vandewater

Copy Editor
Kim Wimpsett

Proofreader
Debbye Butler

Indexer
Potomac Indexing, LLC

Cover Designer
Wiley

Cover Image
©igoriss/iStockphoto

Acknowledgments

First of all, I have to thank Jim for seeing my potential and making the ask. Second, thanks to Kathi and Emily for your expertise and patience. I think we made a great team!

To Eric and Spencer, thank you for the green light as well as Josh, the best sounding board.

To my besties Ryan and Tiffany, I love y'all. We are coming down for chicken wings soon!

Shannan, my sister from another mister, you are my original ripple person. Thank you for believing in me and throwing the rock. You didn't know what you started.

Magen, you have no idea just how inspiring you are.

To Nathan and Ajay, we have gone in different directions and yet we're all still teaching. We have been through some stuff and look how strong it has made us.

Rob, aka CrazyTalk, sudo make me a sammich! Thank you for explaining hashes to me.

Nicole, you are the ying to my yang. I'm always pulling up my bootstraps and asking W.W.N.D.

Lisa, you are one of the most patient, loving people I know. Thank you for being patient and loving me. Julie, thank you for being the most amazing mentor and dearest friend.

Contents at a glance

Contents

Foreword

The year was 2012 and I took a big leap in my own career to move across the country. I filled a role to lead a three-person team providing information technology and security training to Department of Defense personnel. This leadership role was new to me having worked for the past eight years in the intelligence and information security world for the most part as a trainer. While building out the team in the fall of 2012, I interviewed a wonderful candidate from Louisiana named Nadean Tanner. She was full of personality, charisma, knowledge, and most importantly, she had the ability to train. She proved this as part of her training demonstration in the interview process. I knew she was the right candidate and hired her almost immediately. Hiring Nadean is still one of the best decisions I made, and she is one of the greatest trainers I know. My philosophy is that a great trainer does not simply regurgitate what they know. Rather, they have the ability to explain a topic in different ways so that each learner can comprehend. Nadean embodies this philosophy.

Nadean has trained thousands of learners on topics from hardware to advanced security. In each class, she takes the time and effort to ensure every learner gets what they need. Whether learning a product for performing their job, building out their professional development, or advancing their career with a certification, Nadean covers it all. If you had the opportunity to attend one of her training classes, consider yourself blessed by a great trainer. If you have not, you picked up this book, which is the next best thing. I am glad to see her move to authorship, allowing everyone to experience her ability to explain complicated topics in simple ways.

In the world of cybersecurity we are constantly bombarded with new products, new tools, and new attack techniques. We are pulled daily in multiple directions on what to secure and how to secure it. In this book, Nadean will break down fundamental tools available to you. This includes general IT tools used for troubleshooting, but ones that can also help the security team understand the environment. She will cover tools attackers use, but also empower you and your team to use them to be proactive in your security. Specifically, you as the reader get to enjoy not only Nadean's ability to impart knowledge but her uncanny ability to explain why. Rather than being technical documentation focusing on the how, Nadean will delve into why use the tools and the specific use cases. For many users fresh to the cybersecurity world, this should be considered a getting started guide. For those in the middle of or more senior in their careers, this book will serve as a reference guide you want to have on your desk. It is not a book that makes it to your shelf and collects dust.

Throughout the years I have been Nadean's manager, colleague, peer, and most importantly dear friend. We have shared stories about how we learned, what we learned, and how we passed the information along to our learners. As the owner of this book, you are well on your way to enjoying Nadean's simple yet thorough explanations of advanced security topics. Rather than spending more of your time on reading this foreword, jump into the book to learn, refresh, or hone your cybersecurity skills.

Ryan Hendricks, CISSP
Training Manager, CarbonBlack

Introduction

"The more you know, the more you know you don't know."

—Aristotle

"If you can't explain it simply, you don't understand it well enough."

—Einstein

If you have ever been a fisherman or been friends with or related to a fisherman, you know one of their favorite things is their tackle box . . . and telling stories. If you ask a question about anything in that tackle box, be prepared to be entertained while you listen to stories of past fishing expeditions, how big was the one that got away, the one that did get caught, and future plans to use certain hooks, feathers, and wiggly things. A great fisherman learns to adapt to the situation they are in, and it takes special knowledge of all the fun things in that tackle box—when and where and how to use them—to be successful in their endeavor.

In cybersecurity, we have our own form of a tackle box. We have our own versions of wiggly things. To be successful, we have to learn when and where and how to use our tools and adapt to the technical situation we find ourselves in. It can take time to develop the expertise to know when to use which tool, and what product to find vulnerabilities, fix them, and, when necessary, catch the bad guys.

There are so many philosophies, frameworks, compliances, and vendors. How do you know when to use which wiggly thing? Once you know which wiggly thing to use, how do you use it? This book will teach you how to apply best-practice cybersecurity strategies and scenarios in a multitude of situations and which open source tools are most beneficial to protect our dynamic and multifaceted environments.

This book will take a simple and strategic look at best practices and readily available tools that are accessible to both cybersecurity management and hands-on professionals—whether they be new to the industry or simply are looking to gain expertise.

CHAPTER

1

Fundamental Networking and Security Tools

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Ping
- IPConfig
- Tracert
- NSLookup
- NetStat
- PuTTY

Before heading off to the cybersecurity conference Black Hat in Las Vegas, a friend of mine, Douglas Brush, posted on his LinkedIn page a warning for other InfoSec professionals. He said, “Don’t go to these events to buy curtains for the house when you don’t have the concrete for the foundation poured yet.”

Too many times in the many years I’ve been in information technology (IT), I have seen people forget they need the basics in place before they try to use their shiny new tools. Before you can use any new tools, you must have a foundation to build upon. In IT, these tools are fundamental. They are a must for any computer/InfoSec/analyst to know how to use and when to use them. It’s also rather impressive when a manager who you assumed was nontechnical asks you to ping that asset, run a tracert, and discover the physical and logical addresses of the web server that is down. Sometimes they *do* speak your language!

Ping

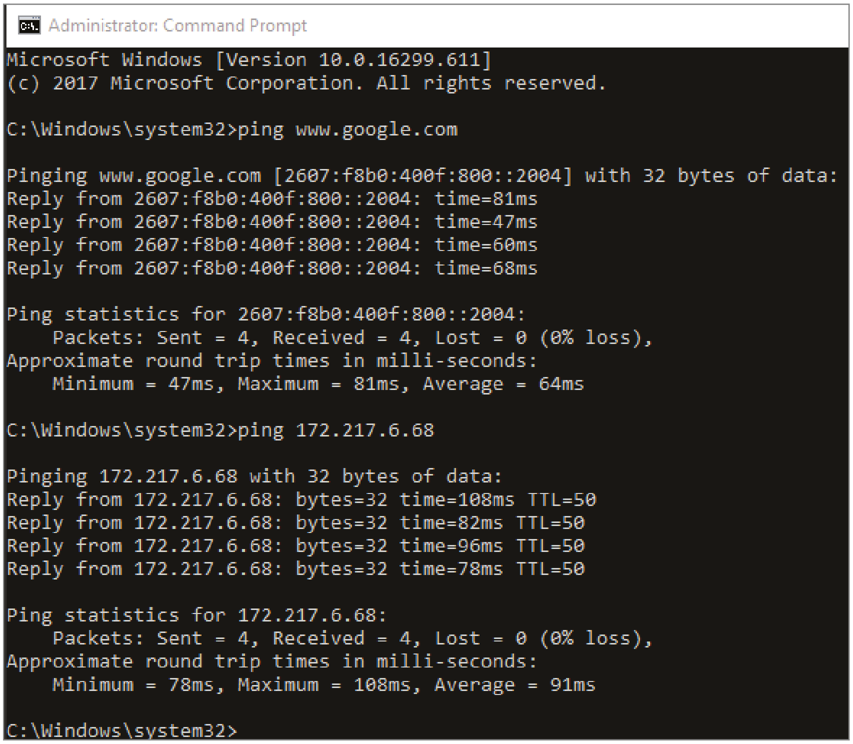
Ping will make you think one of two things. If it makes you think of irons and drivers and 18 holes of beautiful green fairway, then you are definitely CIO/

CEO/CISO material. If it makes you think of submarines or bats, then you're probably geekier like me.

Packet InterNet Groper, or what we affectionately call *ping*, is a networking utility. It is used to test whether a host is "alive" on an Internet Protocol (IP) network. A host is a computer or other device that is connected to a network. It will measure the time it takes for a message sent from one host to reach another and echo back to the original host. Bats are able to use *echo-location*, or bio sonar, to locate and identify objects. We do the same in our networked environments.

Ping will send an Internet Control Message Protocol (ICMP) echo request to the target and wait for a reply. This will report problems, trip time, and packet loss if the asset has a heartbeat. If the asset is not alive, you will get back an ICMP error. The command-line option for ping is easy to use no matter what operating system you are using and comes with multiple options such as the size of the packet, how many requests, and time to live (TTL) in seconds. This field is decremented at each machine where data is processed. The value in this field will be at least as great as the number of gateways it has to hop. Once a connection is made between the two systems, this tool can test the latency or the delay between them.

Figure 1.1 shows a running ping on a Windows operating system sending four echo requests to `www.google.com` using both IPv4 and IPv6.



```
Microsoft Windows [Version 10.0.16299.611]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping www.google.com

Pinging www.google.com [2607:f8b0:400f:800::2004] with 32 bytes of data:
Reply from 2607:f8b0:400f:800::2004: time=81ms
Reply from 2607:f8b0:400f:800::2004: time=47ms
Reply from 2607:f8b0:400f:800::2004: time=60ms
Reply from 2607:f8b0:400f:800::2004: time=68ms

Ping statistics for 2607:f8b0:400f:800::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 81ms, Average = 64ms

C:\Windows\system32>ping 172.217.6.68

Pinging 172.217.6.68 with 32 bytes of data:
Reply from 172.217.6.68: bytes=32 time=108ms TTL=50
Reply from 172.217.6.68: bytes=32 time=82ms TTL=50
Reply from 172.217.6.68: bytes=32 time=96ms TTL=50
Reply from 172.217.6.68: bytes=32 time=78ms TTL=50

Ping statistics for 172.217.6.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 108ms, Average = 91ms

C:\Windows\system32>
```

Figure 1.1: Running a ping against a URL and IP address

What this figure translates to is that my computer can reach through the network and touch a Google server. The `www.google.com` part of this request is called a *uniform resource locator* (URL). A URL is the address of a page on the World Wide Web (WWW). The numbers you see next to the URL is called an *IP address*. Every device on a network must have a unique IP network address. If you are attempting to echo-locate another host, you could substitute the URL `www.google.com` for an IP address. We will do a deeper dive on IPv4 and IPv6 in Chapter 9, Log Management.

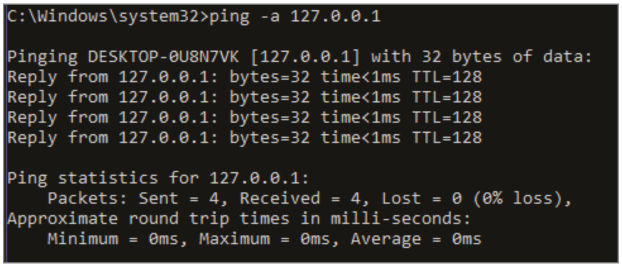
There are more granular `ping` commands. If you type **`ping`** along with an option or switch, you can troubleshoot issues that might be occurring in your network. Sometimes these issues are naturally occurring problems. Sometimes they could signal some type of attack.

Table 1.1 shows different options you can add to the base command `ping`.

Table 1.1: `ping` command syntax

OPTION	MEANING
`/?`	Lists command syntax options.
`-t`	Pings the specified host until stopped with Ctrl+C. `ping -t` is also known as the *ping of death*. It can be used as a denial-of-service (DoS) attack to cause a target machine to crash.
`-a`	Resolves address to hostname if possible.
`-n count`	How many echo requests to send from 1 to 4.2 billion. (In Windows operating systems, 4 is the default.)
`-r count`	Records route for count hops (IPv4 only). The maximum is 9, so if you need more than 9, `tracert` might work better (covered later in the chapter).
`-s count`	Timestamp for count hops (IPv4 only).
`-i TTL`	Time to live; maximum is 255.

Did you know that you could ping yourself? Figure 1.2 shows that 127.0.0.1 is a special reserved IP address. It is traditionally called a *loopback address*. When you ping this IP address, you are testing your own system to make sure it is working properly. If this IP doesn't return an appropriate response, you know the problem is with your system, not the network, the Internet service provider (ISP), or your target URL.



```
C:\Windows\system32>ping -a 127.0.0.1

Pinging DESKTOP-0U8N7VK [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 1.2: Pinging a lookback address