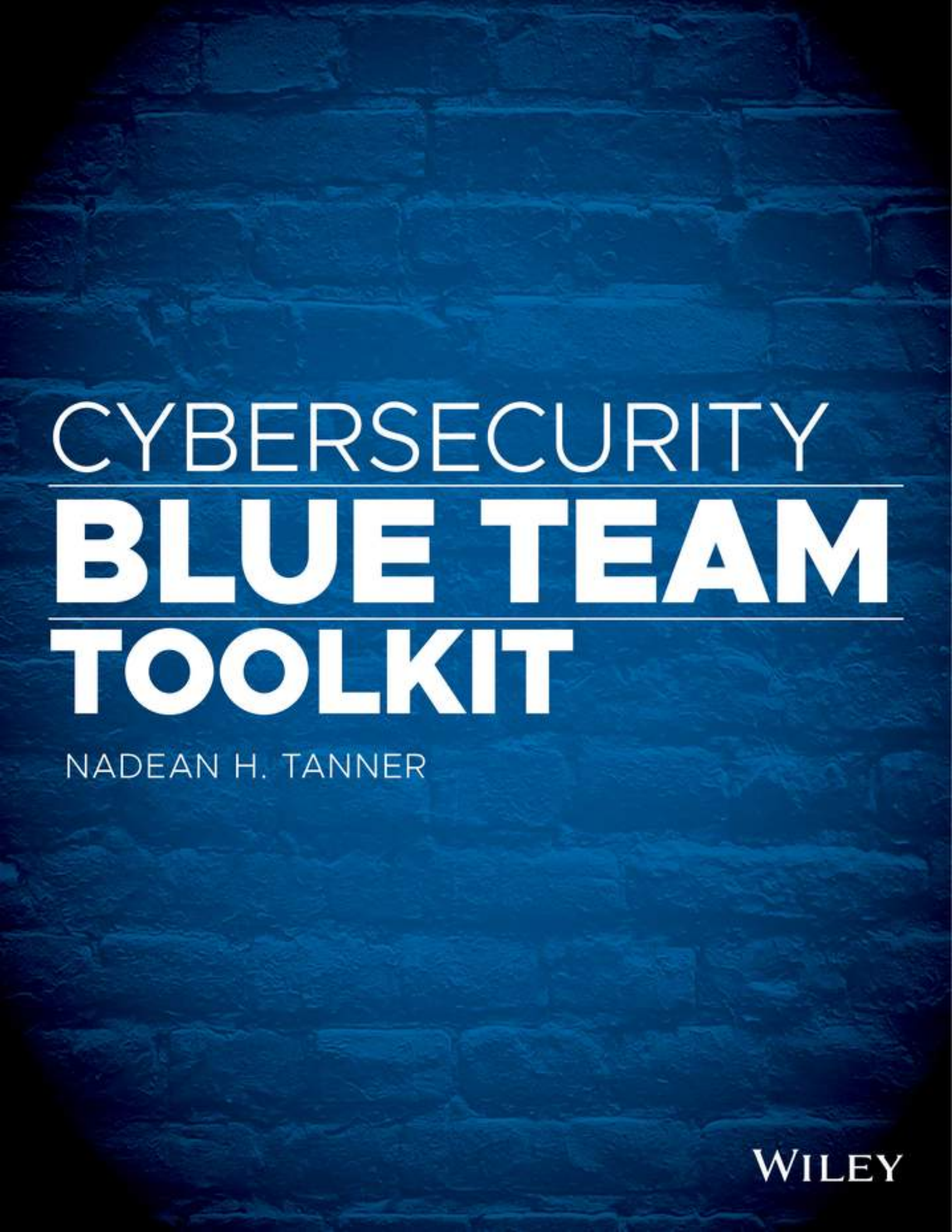




CYBERSECURITY **BLUE TEAM** **TOOLKIT**

NADEAN H. TANNER

WILEY

Table of Contents

[Cover](#)

[Foreword](#)

[Introduction](#)

[CHAPTER 1: Fundamental Networking and Security Tools](#)

[Ping](#)

[IPConfig](#)

[NSLookup](#)

[Tracert](#)

[NetStat](#)

[PuTTY](#)

[CHAPTER 2: Troubleshooting Microsoft Windows](#)

[RELI](#)

[PSR](#)

[PathPing](#)

[MTR](#)

[Sysinternals](#)

[The Legendary God Mode](#)

[CHAPTER 3: Nmap—The Network Mapper](#)

[Network Mapping](#)

[Port Scanning](#)

[Services Running](#)

[Operating Systems](#)

[Zenmap](#)

[CHAPTER 4: Vulnerability Management](#)

[Managing Vulnerabilities](#)

[OpenVAS](#)

[Nexpose Community](#)

CHAPTER 5: Monitoring with OSSEC

Log-Based Intrusion Detection Systems

Agents

Log Analysis

CHAPTER 6: Protecting Wireless Communication

802.11

inSSIDer

Wireless Network Watcher

Hamachi

Tor

CHAPTER 7: Wireshark

Wireshark

OSI Model

Capture

Filters and Colors

Inspection

CHAPTER 8: Access Management

AAA

Least Privilege

Single Sign-On

JumpCloud

CHAPTER 9: Managing Logs

Windows Event Viewer

Windows PowerShell

BareTail

Syslog

SolarWinds Kiwi

CHAPTER 10: Metasploit

Reconnaissance

Installation

<u>Gaining Access</u>
<u>Metasploitable2</u>
<u>Vulnerable Web Services</u>
<u>Meterpreter</u>
<u>CHAPTER 11: Web Application Security</u>
<u>Web Development</u>
<u>Information Gathering</u>
<u>DNS</u>
<u>Defense in Depth</u>
<u>Burp Suite</u>
<u>CHAPTER 12: Patch and Configuration Management</u>
<u>Patch Management</u>
<u>Configuration Management</u>
<u>Clonezilla Live</u>
<u>CHAPTER 13: Securing OSI Layer 8</u>
<u>Human Nature</u>
<u>Human Attacks</u>
<u>Education</u>
<u>The Social Engineer Toolkit</u>
<u>CHAPTER 14: Kali Linux</u>
<u>Virtualization</u>
<u>Optimizing Kali Linux</u>
<u>Using Kali Linux Tools</u>
<u>CHAPTER 15: CISv7 Controls and Best Practices</u>
<u>CIS Basic Controls—The Top Six</u>
<u>In Conclusion</u>
<u>Index</u>
<u>End User License Agreement</u>

List of Tables

Chapter 1

[Table 1.1: ping command syntax](#)

Chapter 3

[Table 3.1: Top Ports Defined](#)

Chapter 4

[Table 4.1: CVSS v3.0 Ratings](#)

Chapter 6

[Table 6.1: IEEE 802.11 standards](#)

[Table 6.2: Wireless Network Watcher command-line options](#)

Chapter 7

[Table 7.1: Keyboard shortcuts for Wireshark](#)

[Table 7.2: Filter operators](#)

[Table 7.3: Expert Info severity levels](#)

Chapter 9

[Table 9.1: Ports used by Kiwi Syslog Server](#)

Chapter 14

[Table 14.1: Resource requirements for Windows 10, Ubuntu, and Kali Linux](#)

List of Illustrations

Chapter 1

[Figure 1.1: Running a ping against a URL and IP address](#)

[Figure 1.2: Pinging a lookback address](#)

[Figure 1.3: Using ipconfig /all](#)

[Figure 1.4: Using nslookup](#)

[Figure 1.5: Using nslookup on a URL](#)