Max Capture: Know Your Packets

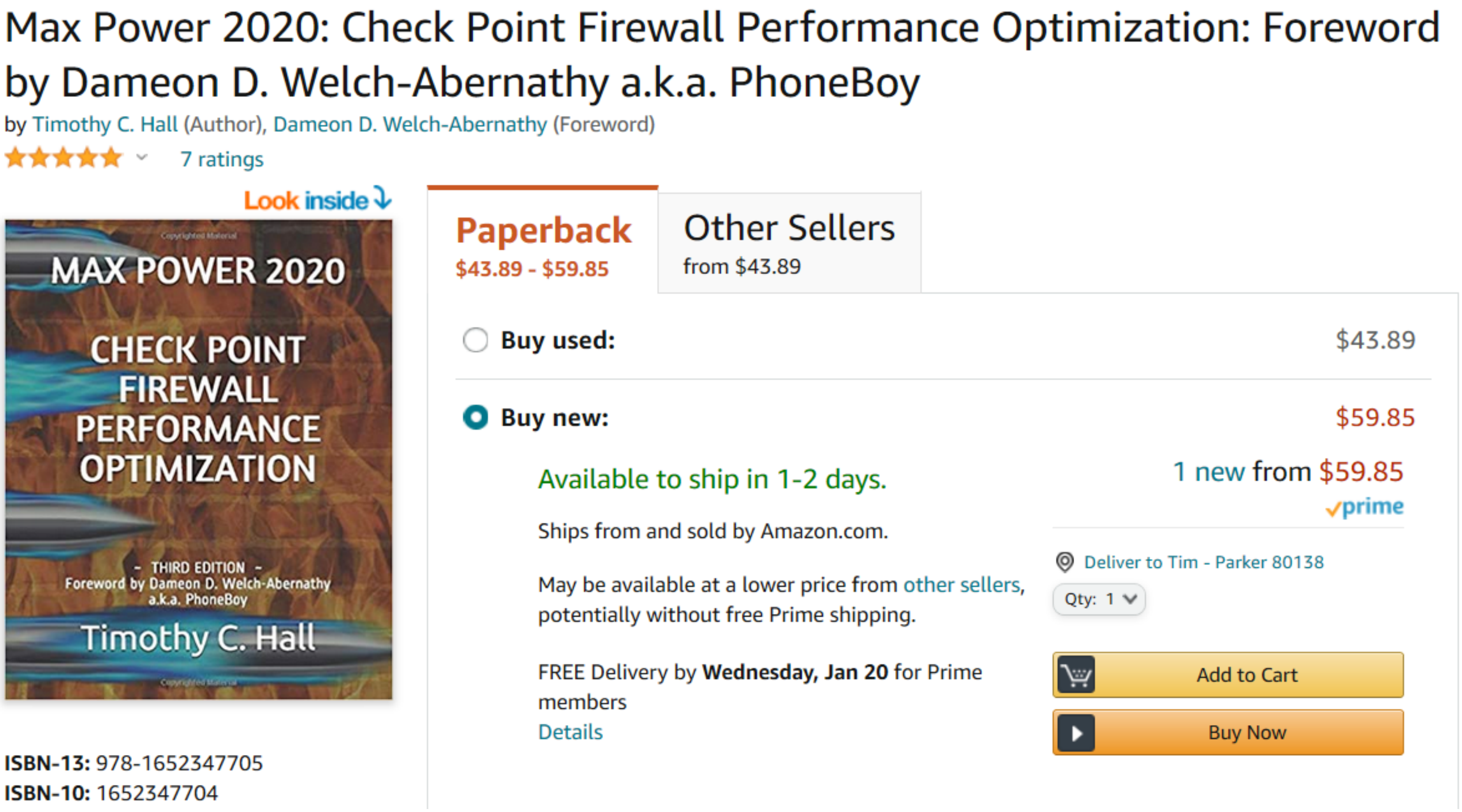
Shadow Peak

SECURITY TRAINING AND SERVICES

Copyright 2021 Shadow Peak Inc. All rights reserved.

Welcome & Introduction

- Your Instructor: **Timothy Hall, CISSP**
  - Worked with Check Point products since 1997, Check Point certified instructor since 2004
  - Founder of Shadow Peak, a Check Point Authorized Training Center (ATC) (http://www.shadowpeak.com)
  - Link to 2,100+ CheckMates Posts   Link to 2,200+ CPUG Posts
  - Author of Book “Max Power 2020: Check Point Firewall Performance Optimization”



Max Power 2020: Check Point Firewall Performance Optimization: Foreword by Dameon D. Welch-Abernathy a.k.a. PhoneBoy

by Timothy C. Hall (Author), Dameon D. Welch-Abernathy (Foreword)

★★★★★ 7 ratings

Look inside
MAX POWER 2020
CHECK POINT FIREWALL PERFORMANCE OPTIMIZATION
- THIRD EDITION -
Foreword by Dameon D. Welch-Abernathy a.k.a. PhoneBoy
Timothy C. Hall

ISBN-13: 978-1652347705
ISBN-10: 1652347704

Paperback $43.89 - $59.85 | Other Sellers from $43.89

○ **Buy used:** $43.89

● **Buy new:** $59.85

Available to ship in 1-2 days.

Ships from and sold by Amazon.com.

May be available at a lower price from other sellers, potentially without free Prime shipping.

FREE Delivery by **Wednesday, Jan 20** for Prime members
Details

1 new from $59.85
✓prime

Deliver to Tim - Parker 80138

Copyright 2021 Shadow Peak Inc. All rights reserved.

Table of Contents

Welcome & Introduction........2
Max Capture: Know Your Packets Class Details........6
Module 1 – How Can Packet Captures Help? Or Not........7
What Packet Captures Can Do........7
What Packet Captures CAN'T Do........8
Summary........8
Module 2 – Little-known Alternatives to Packet Captures........9
"Accounting" Logging Option........9
Is There an Equivalent to Cisco's "Packet Tracer" tool? Yes and No........13
Traffic Crafting........13
Policy & NAT Testing........15
Routing Test........18
TCP State Logging........19
TCP State Logging Example Screenshots........21
SmartConsole GUI "Capture Packets" Option........24
Summary........27
Module 3 – The Basics: fw monitor, tcpdump, & cppcap........28
fw monitor -e........28
fw monitor -F........29
tcpdump........30
cppcap........31
Special Case: Scalable Platforms/Maestro........32
Regardless of the Capturing Tool Selected...Look Out!........32
fw monitor and its "Capture Points"........33
SecureXL and How It Impacts Taking Captures........35
Capture Point Positioning of the Four Tools........38
Module 4 – Table Comparing and Contrasting the Four Capturing Tools........41
Tool Comparison Table Notes........42
Tool Conversion Table for Command-line Switches........46
Useful tcpdump Command-line Switches........47
Useful fw monitor Command-line Switches........48

Copyright 2021 Shadow Peak Inc. All rights reserved.

Useful cppcap Command-line Switches........49
Overall Capture Tool Recommendations........50
Module 5 – Some Cautions & Direct CLI Analysis of Captures........51
Beware: TCP port 22 and UDP port 8116........51
Beware: The "Observer Effect"........52
Beware: Security Acceleration Module (SAM) Ports........53
Beware: Typos in Capturing Filters: Especially fw monitor -F........54
Command-Line Output Formats of the Various Tools........57
Unfiltered Capture Use Case & Examples........59
Lab 1: Packet Capture CLI-based Analysis........62
Module 6 – Enough Theory...Let’s See Some Real Filtering Examples!........64
Module 7 – Advanced CLI Troubleshooting with Packet Captures........74
Special Case: Following NATted Traffic UUID with fw monitor -e........74
Special Case: Following NATted Traffic with fw monitor -F........76
A Neat Trick: Using tcpdump to Troubleshoot Application Performance Problems........76
Cookbook: Troubleshooting the “Roach Motel”........78
Step 1: Verify that Traffic Should be Crossing the Firewall...or Identify the Correct Firewall........79
Step 2: Ensure the Traffic is Actually Reaching the Firewall in the First Place........79
Step 3: Check for Check Point Product Code Drops........81
Step 4: Check for Gaia OS Drops........82
Step 5: The Final Possible “Corner Case” Drops........83
Lab 2: The Dreaded "Roach Motel"........85
Module 8 – Interpreting Packet Captures in Wireshark........86
Saving pcaps and Importing to Wireshark........86
"Live" Wireshark Captures on the Firewall via tcpdump & plink.exe........89
Configuring Wireshark........90
Most Useful Features of Wireshark in the Real World........93
Basic Packet Filtering Syntax........93
Viewing Packet Header Decodes & Raw Bytes........94
Coloring Rules........97
Follow...TCP Stream........102
Marking Packets........103

Copyright 2021 Shadow Peak Inc. All rights reserved.

Network Activity Statistics & Expert Information....105
Lab 3: Pulling Captures into Wireshark for Analysis....112
Module 9 – Beyond the Firewall: Using tcpdump/windump Elsewhere....113
Remotely-Initiated Captures with rpcapd....115
Module 10 – TL;DR: Quick Start Guide for tcpdump....117
Workflow for tcpdump Quick Start....118
Quick Examples of tcpdump Filtering Syntax....120
tcpdump Tips, Tricks, & Best Practices Review....121
Wrap–up Discussion and Additional Resources....123

Copyright 2021 Shadow Peak Inc. All rights reserved.

Max Capture: Know Your Packets Class Details

- Prerequisites: Basic systems and networking knowledge.
- The slides we will be working in the recorded videos are identical to this PDF document provided with the course.
- We will be working with the Gaia OS version associated with the R80.40 release (Red Hat Enterprise Linux [RHEL] 7 with kernel 3.10), but will also mention the older 2.6.18 kernel used in some firewall installations of R80.30 and almost all earlier firewall code releases.
- The main focus of this course is the Gaia 3.10 kernel running on Check Point appliances (models 2200-28XXX), open hardware, and some types of virtualized environments.
- Limitations relevant to Scalable Platforms (models 41000+), Maestro, and VSX will be noted. For Scalable Platforms, the following two SKs are invaluable reading for special troubleshooting tips and techniques unique to these platforms:
  - sk101556: ATRG: 60000 / 40000 Security System
  - sk67142: 60000 / 40000 Appliances - Performance Tests Troubleshooting
- The material presented in this course will mostly apply to CloudGuard gateways (which also utilize the same RHEL7 Gaia 3.10 OS), subject to the specific limitations detailed in sk160753: Check Point R80.40 Known Limitations and to a lesser degree Section 7 of this SK: sk141173: Check Point R80.20 with Gaia 3.10 for CloudGuard and Open Server Security Gateways.
- Note that **tcpdump** and **cppcap** will not work at all on vSEC for NSX-V / vSEC Virtual Edition Hypervisor Mode, use **fw monitor** instead; this limitation only applies to NSX-V, not NSX-T. See sk116796: **'tcpdump' utility does not capture the specified traffic on vSEC for NSX / vSEC** Virtual Edition Hypervisor Mode.
- Embedded Gaia (which is based on the Linux BusyBox OS and utilized on the 600-1800 appliance models) is not explicitly covered in this course, but the concepts and most capture operations should be similar.
- Hyperlinks shown in this document are “hot” and can be clicked to show the specified resource in your web browser.

Copyright 2021 Shadow Peak Inc. All rights reserved.