

---

## Book Review: Practical Packet Analysis, Second Edition

Review by J. Oquendo AKA sil

"Practical Packet Analysis: Using Wireshark to Solve Real World Problems" is a decent book for readers who are relatively new to networking. It makes a great addition for someone in the one-to-three year range of their career. Whether this career is security-centric, network administration, or simply as a hobbyist, Chris Sanders made great work of keeping things simple yet informative for his readers. While this is a plus for the entry person, it is also its minus for the seasoned pro.

The beginning of the book gives an overview of the OSI layer, which I have found many in the IT industry skimp on. Whether you are in networking, systems, programming or the security arena, understanding the interconnections of protocols and how they operate with one another across the layers should be the first and foremost knowledge one should memorize. Because Chris took the time and brought this out at the forefront, it will be beneficial to the reader, which once again I feel would be a junior administrator. Let's get into some more details after the break.

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Book Reviews}

After "Packet Analysis and Network Basics" in Chapter 1, Chris gets briefly into mirroring in Chapter 2, "Tapping into the Wire." Unfortunately there was little mention about VLANs. In an advanced network (and by advanced I mean a network built by someone with experience), there are a lot of caveats. That will frustrate a reader of this book, because there is no mention of VLAN monitoring. Port sniffing VLANs is a different beast with switches offering a variety of different options yielding different output. For example, in my real world, I am not always concerned with Egress traffic. Egress is not even a term used in the book. Nor was say port mirroring across switches, which in the Cisco world would be labeled RSPAN, VSPAN, or PSPAN. While not a big deal for the junior level professional, it makes a world of difference for the seasoned professional.

Chapters 3, "Introduction to Wireshark," and 4, "Working with Captured Packets," introduce or re-introduce the reader to Wireshark on a very basic level. This will include introducing the reader to basic filters, basic

dissectors and a few of the windows available. Chapter 5 is labeled "Advanced Wireshark Features" which is a bit deceptive. Deceptive in the sense that it could have just been included in Chapter 4.

Positioning of Chapters 6 and 7 seem a bit confusing. However, I will call this an obsessive compulsive point of view. The two chapters consist of upper and lower layer protocols; however, I believe the reader should have read these two chapters before seeing a chapter called "Advanced Wireshark Features." While this is not that big of a deal, the author gives a junior reader some solid information into understanding DHCP, DNS, IP, TCP, UDP, ARP, etc. Some of this information should have probably come after Chapters 1 and 2 before even getting into Wireshark; however, this is how the book flows. It will come in handy for the reader, as they are likely to not be a hardcore network or security engineer.

Chapter 8 seems slightly misplaced because of the naming as well. As a reader, you will see "Advanced" followed by "Basic Real-World Scenarios." In this chapter, the "real world" problems seem to be problems one might see in a very small office of perhaps 10-15 users or on a home network. This is not necessarily a "bad thing" however. Because of the name of the book "Practical Packet Analysis," I was expecting a little more. But it does suffice for some simple practical examples.

Chapter 9, "Fighting a Slow Network," gives a brief overview of troubleshooting latency issues but is focused almost exclusively on TCP. The chapter is informative for someone new to troubleshooting and will be very helpful to up and coming administrator. However, following this chapter as any kind of de-facto standard would be a bit disastrous. In almost all networks I have had my hands in over the years, it pays to focus on all protocols when trying to determine the cause of latency and bottlenecks. For example, at face value, a reader might interpret this chapter as, "focusing on TCP window sizes, re-transmissions and the likes, will let me know why my network isn't slow." This is not always the case. In fact, even now I still see broadcast storms (a term also not even mentioned in the book) bring networks to a crawl. I have also seen UDP and RTSP streams make networks crawl as well.

By the time I got to Chapter 10 "Packet Analysis for Security," I had been hoping for some meatier security topics, however I was disappointed. The exploitation section titled, "Operation Aurora," seemed based on the author perhaps configuring Metasploit using its "aurora exploit browser module." This, while giving the reader a briefer on browser exploits, can also embed a false sense of relevant information bordering on misleading. Because most of us learn by the writings and explanations of others, the reality behind Aurora was that it tunneled data through HTTPS (port 443) and used its own substitution and encoding to avoid detection as described in the Power Source Online article, Operation Aurora Attacks. Personally, I believe the author misleads anyone trying to get into the security arena by throwing out the term "Operation Aurora." Or maybe a little better technical editing was required.

To be quite candid and fair, Chris Sanders's Practical Packet Analysis published by No Starch Press is a good book for someone new to networking and or security; however, there is a lot of information that this book lacks. Please take note that I am basing my review on experience. In no way, shape or form am I trying to write a scathing review, but if you are planning on getting into serious network analysis and troubleshooting, then this book ranks in what I would say "a slight step up from the For Dummies" series. And at only 280 pages, it totally fits the bill if you need a quick and dirty intro into Wireshark. However, if you plan on using and understanding Wireshark to its maximum capabilities and potential, throw in a few more bucks and get Laura Chappell's "Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide."

J. Oquendo, SGFA, SGFE, C|EH, CNDA, CHFI, OSCP, CPT, RWSP, GREM

Mr. Oquendo has close to 30 years computing. Twenty of these years have been professional with over 14 or so years in security and networking specific roles. His day-to-day duties vary while working for a telecommunications company that is also a Managed Services Provider (MSP). Those services include networking (design, administration, monitoring), VoIP (ITSP, trunking, design, configuration, deployment, management), and security (SIEM, forensics, incident response, penetration testing, vulnerability assessments, application and code auditing). His current position is Chief Security Architect at a company that he discloses to trusted friends and peers.