The Open Pitt

What's cooking in Linux and Open Source in Western Pennsylvania

Issue 33 March 2007 www.wplug.org

Book Review: *Secure Your Network for Free* by Larry Daberko

Author: Eric Seagren
Publisher: Syngress Publishing
ISBN: 1-59749-123-3
$39.95, 493 pages, 2007

Eric Seagren has been a contributing author and technical editor for six other network security books, and this is his first solo work. He's been in the computer industry for 10 years, working for JPMorganChase & Co. for the last eight.

Secure Your Network for Free is written in a clear, easy-to-read style that seems aimed for the novice starting in the security field. Having been involved in network security for a few years, I was already familiar with much of the material. However, this book covers such a wide variety of subjects that even experienced hands will pick up a few new tidbits. This book also keeps in mind the impact and interaction that network security has with the business and user side.

The book's cover features the following security programs: Nmap, Wireshark, Snort, Nessus, and MRTG. (I must have been away from the Internet too long because I didn't realize that Ethereal is now called Wireshark.) But the book doesn't include only these programs—it covers a lot more. Readers will get a broad view of network security which then drills down into concrete examples.

Special Election Ahead

WPLUG will be holding a special election to fill a vacancy in the office of Treasurer.

Nominations will take place at the April meeting. Votes will be counted during the May meeting, and ballots may be mailed in or submitted in person.

Members of WPLUG are eligible to vote and run for the office as governed by the bylaws.

Full details and voting instructions will be sent out to all members.

The chapters are arranged in a logical order, starting with convincing the bosses, then moving on to securing the perimeter, securing the internals, detecting intrusions, keeping logs, auditing, reporting, and continuing the security process.

There were a few pleasant surprises that you might not expect from a technical computer book. The first chapter, Presenting the Business Case for Free Solutions, guides the reader through several examples on what to consider when calculating the “cost” of free solutions, including training, hardware, consulting and hidden costs. People often focus just on the purchase price, but sometimes a “free” software package may end up costing more in wages than a paid-for product if it takes a long time to learn and implement. The book also gives guidelines on how to “sell” a free solution if that evaluates to be the best fit. Sometimes, the bosses need more convincing than we do.

Chapters 2 through 7 constitute the meat of the book, listing programs that can be used in various aspects of the network security system and showing step-by-step instructions for implementing them. Windows and Linux systems seem to be treated equally with examples given for both, and there is an absence of Microsoft bashing. Each chapter ends with a “Solutions Fast Track” which lists major points and a FAQ section giving various questions and answers pertaining to the chapter subject.

Chapter 2, Protecting Your Perimeter, starts by going over firewall types and how to integrate them into your network design. Different DMZ setups are also explained here, and the pros and cons of each design are detailed. The author then rolls right into setting up a firewall such as Netfilter, gives configuration examples, and discusses graphical configuration tools and Smoothwall. As part of protecting the perimeter, secure remote access using various VPNs, remote desktops, and remote shells are described.

Protecting Network Resources, Chapter 3, takes on what many consider to be the “chewy center” of network security. A high-level view of policy-making is covered before diving right into hardening Windows and Linux systems. Patching, implementing personal/host firewalls, antivirus and antispyware are discussed as well. The author also includes Windows' Encrypting File System.

What do you do after securing the network? You gotta watch it, which is the subject of Chapter 4, Configuring an Intrusion Detection System. After an overview of hardware requirements and where to place them, the book goes through configuring Snort on Windows and Linux and mentions some add-ons. One bit of good advice Seagren gives is to place an IDS outside the firewall in order to demonstrate how effective the network security is. There's nothing like showing your boss thousands of rejected hack attempts to make you and your investment in security look good.

See **SECURE**, *p. 2*

Coming Events

Apr. 14: General User Meeting. *(Time and location TBA, see web site for details)*

The public is welcome at all events

From the Editor: It's Hard(ware)

Dell Computer, the giant supplier of desktop, laptop, and server systems recently established its IdeaStorm web site to ask people what they want. In huge numbers, the answer was—Linux on Dell equipment. Dell initially said it would “certify” particular models to work with Novell's SUSE Linux. It quickly became clear that this was not sufficient and that people wanted systems pre-installed with Linux instead, and it now appears that Dell will try to meet that demand.

While an interesting tale in its own right, it becomes even more so when viewed in its larger context. Quanta Computing, which manufactures laptops for companies like HP, Dell, and Acer and which is producing the One Laptop per Child (OLPC) device, is considering making a low-cost laptop running Open Source software based on its OLPC experience.

It seems clear that hardware suppliers are facing increasing pressure to develop a Linux and Free Software strategy. Taking into consideration Greg Kroah-Hartman's standing offer `<http://kerneltrap.org/node/7636>` to develop Linux drivers for hardware manufacturers' devices, there is no longer any technical reason not to make your hardware work with Linux.

The result of Dell's experiment will serve as an indicator of whether other, more business-related factors point in favor of supporting Linux. While some niche players have achieved success with Linux, you can bet that system and device manufacturers across the globe will be looking to these large-scale examples from the likes of Dell and Quanta when deciding on their own strategies. If successful, we may see a tsunami as others rush to follow.

SECURE, *from p. 1*

Chapter 5 deals with Managing Event Logs. It first goes into setting up Windows to generate logs before diving into syslog. Several utilities that can convert Windows event logs to syslog messages are mentioned. Linux syslog is covered also. In addition to analyzing logs, the author explains the importance of maintaining their integrity. He gives tips on how to make your logs stand up to legal scrutiny by securing them and making sure they don't change by using checksums.

The next chapter gets into what I think is the fun part, Testing and Auditing Your Systems. Inventorying the network is demonstrated using various scanning and testing programs such as Nmap, SuperScan, Angry IP Scanner, and ScanLine. Network Stumbler (aka NetStumbler) is also shown for locating wireless networks. Network documentation including topology maps, policies, and disaster recovery plans are briefly touched on before getting into the actual vulnerability scanning. Nessus on Linux and Windows, X-Scan, and Microsoft Baseline Security Analyzer are covered. The author also gives a brief recommendation of the Open Source Security Testing Methodology Manual (OSSTMM).

Chapter 7, Network Reporting and Troubleshooting, goes over monitoring bandwidth using SNMP and graphing with MRTG, TrafficStatistic, PRTG, or ntop. Troubleshooting is covered using Wireshark, WinDump, tcpdump, and ngSniff.

The last chapter, Security as an Ongoing Process, shows how to maintain the secure environment after implementation is done. It includes patch and change management and explains about keeping antivirus, spyware, vulnerability scanning, and intrusion detection systems up to date. It also goes into a general overview of miscellaneous items that didn't fit anywhere else.

Secure Your Network for Free does try to balance broad coverage of the network security job with depth in the program examples to fit the differing experience levels of various readers. I would recommend this book to someone newly interested or starting off in the network security field. More experienced users might pick up a few ideas like I did by skimming through the book, but in the end they are likely to want a more advanced text.

Larry Daberko is a network administrator who mainly uses BSD but has been dabbling in Linux, Cisco, and Windows for about 15 years. “Jack of all trades, master of none, though ofttimes better than master of one.”

The Open Pitt is published by the Western Pennsylvania Linux Users Group
`<http://www.wplug.org/top/>`

Editor: Vance Kochenderfer

What is Linux?

Linux is a *kernel*, the core of a computer operating system, created by Linus Torvalds. It is typically packaged as a *distribution*, which includes the extra programs necessary to make a computer functional and useful. Since 1991, it has grown from a one-man project which ran on one computer to one with thousands of contributors running on everything from personal organizers to million-dollar supercomputers.

What are Open Source and Free Software?

Open Source and Free Software provide you, the user, with the opportunity to see the source code of the programs you use. You are free to use it, share it with others, and even make changes to it if you wish. While the Free Software and Open Source communities differ in their philosophical approach, in practical terms they share nearly identical goals. Learn more at `<http://www.opensource.org/>` and `<http://www.gnu.org/>`.

This newsletter was produced using Open Source and Free Software.