Book Review: Linux Firewalls - Attack Detection and Response with iptables, psad, and fwsnort

By *srlinuxx*
Created *28/11/2007 - 12:28am*
Submitted by srlinuxx on Wednesday 28th of November 2007 12:28:45 AM

Working in a university environment, one gets used to doing more with less. Security, particularly, seems to never get the budget it deserves though it has increased in recent years. For all their limitations, open-source tools are the vital lifeblood that makes IT work, and work securely, in academia.

Using Netfilter (or commonly called iptables) for the firewalls have managed to reduce costs but provide stable and secure service to the users. However, for some time we've been looking to get more out of our firewalls to enhance the security and data reporting from the firewalls. The syslogs are all fine and good, but no one is seriously going to review them without some application doing the heavy lifting of making the data presentable.

Linux Firewalls, in this regard, is a great resource. It provided insight and helpful information into additional tools to get the most out of iptables and to add in additional functionality. The book covers basic iptables fundamentals and then covers the additional applications of psad, fwsnort, fwknop and data visualization of firewall logs.

More Here [1]

Links:
[1] http://blogcritics.org/archives/2007/11/27/075042.php