

Re: Data Mining for PIX Firewall Logs

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0067.html>

From: Michael J McCafferty (*mike_at_m5computersecurity.com*)

Date: 02/11/05

Date: Fri, 11 Feb 2005 07:18:26 -0800

To: pen-test@securityfocus.com

PIX firewalls log in syslog format to a syslog server. Syslog is a Unix application. Unix (and Unix like OSes like Linux, BSD, etc) machines have other utilities on them that make searching through a text log file like those created by syslog a breeze. But since you are using Kiwi, that tells me you are logging to a Windows machine. It's unfortunate that Windows machines to this day still do not offer a good way to parse through text log files. The right tool is a Unix box.

There are some options for you.

- 1) You can install those tools that one would usually use on a *nix system, which have been ported to Windows. Try Cygwin, for example. There are other ports of the tools like grep, tail, less, more, cat, awk, etc. to Win32. Cygwin may be the most comprehensive. <http://www.cygwin.com/>
- 2) Log to a Unix syslog server and use those tools natively. There are several free OSes that you can stick on that same hardware that you are using Windows on now. Logging doesn't require much horsepower at all. Consider Fedora Core (what used to be RedHat), you can get lots of help from other Linux newbies. <http://fedora.redhat.com>
- 3) Use the Kiwi Logfile Viewer. I have not used it. Never seen it. It's on the Kiwi web site. <http://www.kiwisyslog.com/>

If you want to tip-toe in to option 2 above, you can set your PIX to log to two locations. Grab an old PC, and set up a second log server to try option 2 above. There is no doubt gonna be a learning curve to using the basic Unix tools, like grep, awk, tail and less.... and navigating around the new OS... if you are a total newbie to Unix or Linux. If you are not, then I guess you are not likely to have asked this question in the first place. :o)

You will also need to set up your logs to rotate on your new OS. Your log rotation script can compress the logs and you can archive these logs for as long as you have disk space. You can search compressed logs with something like "zcat logfile.gz | grep <pattern>"

SecurityFocus Penetration: Re: Data Mining for PIX Firewall Logs

Good Luck, you have some fun learnin' ahead of you,
Mike

At 05:08 PM 2/9/2005 -0500, Carey Heck wrote:

>Hi folks. I love the ability in the Checkpoint firewall logging
>applet that allows me to load up any former saved log file, and filter
>according to any criteria I set.
>
>Lets use an example:
>
>I want to show an auditor what exactly went through my firewall,
>to/from a specific DMZ host, between the hours of 1 and 3pm GMT, on
>July 8th, 2003.
>
>In checkpoint, if I had correctly configured my ruleset, and archived
>my log files properly, I could provide this answer within 30 minutes.
>
>Fast forward to my current company, which went with a Cisco PIX
>solution based on the up front cost. I can log all the connections to
>my heart content, but boy mining the data to help show what happened
>in my above example has been tiresome at best.
>
>Can anyone here please suggest to me some type of logging and more
>relevantly, a data mining product that can help me achieve this end?
>
>Currently I am logging all my PIX traffic to a host running Kiwi
>syslog daemon, which archives each days logs into a separate folder in
>the dated logs directory, creating a new directory named for each date
>in the year.
>
>I am looking for a less clunky solution.
>
>Any help is GREATLY appreciated.
>
>Thanks!
>
>--
>Carey

Michael J. McCafferty
Principal, Security Engineer
M5 Hosting
<http://www.m5hosting.com>

Think of the fun you could have with a M5 Hosting Dedicated Server !
OpenBSD, Fedora, RHEL, Debian, FreeBSD, and more
