

Re: Automated analysis of logs?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-04/0151.html>

From: Tomasz Onyszko (T.Onyszko@w2k.pl)

Date: 04/09/03

From: "Tomasz Onyszko" <T.Onyszko@w2k.pl>

To: <security-basics@securityfocus.com>

Date: Wed, 9 Apr 2003 20:12:28 +0200

W dniu Tuesday, April 08, 2003 7:27 PM [GMT+1=CET],

Mark G. Spencer <mspencer@evidentdata.com> napisa³:

Hi

- > *Are there any open-source applications that I can drop various kinds*
- > *of logs*
- > *into (especially IIS logs) and get not only statistics, but*
- > *information*
- > *and/or "warnings" about various kind of known activity? Things like (...)*

- > *I know some people are more proactive about this and stick a Snort box*
- > *upstream, but in most cases I am responding to an event where the*
- > *deed has*
- > *been done and I can't go back in time, so I only have logs available*
- > *to me.*
- >
- > *If there are no OS solutions, is there a well regarded commercial*
- > *product*
- > *that can do this?*

I've found lately a tool from Microsoft called LogParser which I think can be helpful for You. This tool allows You to query log files in SQL way and save output in some various format like XML, IIS log or directly to the SQL database table. I think Log Parser connected with SQL server and some batch files let You develop some custom log analysis solution. LogParser can be downloaded from this location:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8CDE4028-E247-45BE-BAB9-AC851FC166A4>

Best regards

Tomasz

--

Tomasz Onyszko - T.Onyszko@w2k.pl

<http://www.w2k.pl/>

Is SPAM over-loading your e-mail server, disk space or bandwidth?
SurfControl E-Mail Filter is flexible, intelligent and policy-driven

Re: Automated analysis of logs?

SecurityFocus BASICS: Re: Automated analysis of logs?

protection.

<http://www.securityfocus.com/SurfControl-security-basics2>

Download your free fully functional trial, complete with 30-days of free technical support.
Stop SPAM before it stops you.
