

[TOOL] FWAnalog, Firewall Log File Reporting Tool

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0086.html>

From: support@securiteam.com

Date: 12/20/01

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 20 Dec 2001 17:27:11 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

FWAnalog, Firewall Log File Reporting Tool

DETAILS

FWAnalog is a shell script that parses and summarizes firewall log files.

It currently understands logs from IPF (tested with OpenBSD 2.8 and 2.9's

IPF, also FreeBSD and NetBSD), Linux 2.2 IPChains and Linux 2.4 IPTables.

It has been tested on Debian GNU/Linux "sid" with bash and OpenBSD 2.8 and

2.9 with ksh as /bin/sh.

It can be easily extended for other log file formats; all it takes is editing two regular expressions.

FWAnalog uses the excellent log analysis program Analog (also free software) to create its reports. It does so by converting the firewall log into a fake web server log and calling Analog with a modified configuration.

ADDITIONAL INFORMATION

The tool can be downloaded from:

<<http://tud.at/programm/fwalog/>> <http://tud.at/programm/fwalog/>

Securiteam: [TOOL] FWAnalog, Firewall Log File Reporting Tool

The information has been provided by <mailto:balazs@tud.at> Balázs Bárány.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[\[UNIX\] Linux Distributions are Vulnerable to the /bin/login Overflow](#)"
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)