

[TOOL] SnortALog – Snort Analyzer Logs

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0039.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/15/04

To: list@securiteam.com

Date: 15 Sep 2004 11:05:55 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

SnortALog – Snort Analyzer Logs

SUMMARY

DETAILS

<<http://jeremy.chartier.free.fr/snortalog/>> SnortALog is a powerful perl script that summarizes snort logs making it easy to view any attacks against your network. SnortALog works with all versions of SNORT and is the only script who can analyze snort's logs in all formats (Syslog, Fast and Full alerts). Also, it is able to summarize Fw-1 (NG and 4.1), Netfilter and IPFilter logs in a similar way.

Current Capabilities:

- * Create HTML, PDF and text reports
- * Generate GIF, PNG or JPG graph in HTML output
- * CLI (Command Line Interface) and GUI (Graphic User Interface)
- * Works with Syslog, Fast and Full SNORT alerts
- * Works with all SNORT preprocessor (spp_stream4, spp_portscan, spp_decoder, flow, flow-portscan ...)
- * Has the possibility to link the SNORT signature to the web reference attack description
- * Works with "-I" Snort option to specify an interface and add report
- * Work now with "-e" Snort option (Display the second layer header info)
- * Use a specific plugin for generate your owns reference's SNORT rules

Securiteam: [TOOL] SnortALog – Snort Analyzer Logs

- * Can specify order (ascending or descending)
- * Can specify the number of occurrences to view
- * Can resolve IP addresses and domains
- * Add colors for a best visibility
- * Possibility to do filtering (if you only want a specific IP source or high severity snort logs)
- * Works with Fw-1 (4.1 and NG) in syslog and fw logexport command
- * Works now with Fw-1 SmartDefense
- * Works with Netfilter and IPFilter syslog logs
- * Works now with syslog PIX log(Thanks to Edwin)
- * Possibility to use DBM
- * Works on Windows box (basic option: no graph)

Download Information:

To obtain the latest version of the tool see:

<<http://jeremy.chartier.free.fr/snortalog/#download>>
<http://jeremy.chartier.free.fr/snortalog/#download>

ADDITIONAL INFORMATION

To keep updated with the tool visit the project's homepage at:

<<http://jeremy.chartier.free.fr/snortalog/>>
<http://jeremy.chartier.free.fr/snortalog/>

=====

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.