

[TOOL] L7-Filter – Application Layer Packet Classifier for Linux

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0117.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/25/05

To: list@securiteam.com

Date: 25 Jan 2005 18:42:59 +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>

L7-Filter – Application Layer Packet Classifier for Linux

SUMMARY

DETAILS

This is a classifier for the Linux kernel's Netfilter subsystem that identifies packets based on application layer data (OSI layer 7). This means that it can classify packets as HTTP, FTP, Gnucleus, eDonkey2000, etc, regardless of port. Our classifier complements existing ones that match on address, port numbers and so on.

The developer's intent is for l7-filter to be used in conjunction with Linux QoS to do bandwidth arbitration ("packet shaping").

Feature Overview:

- * Patches for Linux 2.4 and 2.6
- * Support for TCP, UDP and ICMP over IPv4
- * Uses Netfilter's connection tracking of FTP, IRC, etc
- * Examines data across multiple packets
- * Number of packets examined tunable through `/proc/net/layer7_numpackets`
- * With the Netfilter helper match, can distinguish between parent (ex. ftp command) and child (ex. ftp data) connections

Securiteam: [TOOL] L7-Filter – Application Layer Packet Classifier for Linux

- * Gives access to both Netfilter (firewall) and QoS (rate limiting) features
- * Might be in the stock kernel, or at least patch-o-matic, some day

ADDITIONAL INFORMATION

The information has been provided by Ethan Sommer and Matthew Strait.
To keep updated with the tool visit the project's homepage at:
<<http://l7-filter.sourceforge.net/>> <http://l7-filter.sourceforge.net/>

=====

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.