

[TOOL] HLBR – Open Source Intrusion Prevention System

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00023.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 8 Mar 2006 16:16:19 +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>

HLBR – Open Source Intrusion Prevention System

SUMMARY

DETAILS

IPS HLBR – Version 1.0 can detect malicious traffic using regular expressions

Version 1.0 of Hogwash Light BR, released march 5th 2006, brings two interesting new features. The first one is the ability of using regular expressions to detect intrusion attempts and e-mails with viruses or phishing. The second is the use of lists with banned words.

HLBR is an IPS (Intrusion Prevention System) that reads network traffic in the layer 2 of the OSI model. Since it works like a bridge, it stays in-line in the network topology and doesn't need an IP address. So, HLBR is invisible to attackers. Traffic filtering (including the packets contents) can be done with simple rules. Version 1.0 can use regular expressions to filter the packets. Below is an example of rule with regular expressions:

[TOOL] HLBR – Open Source Intrusion Prevention System

<<http://hlbr.sourceforge.net/hlbr-rule-1.gif>>
<http://hlbr.sourceforge.net/hlbr-rule-1.gif>

In short, all TCP traffic destined to port 25 of the e-mail server will be filtered. If the text:
filename="anything_different_of_line_breaks.s__c__r" (ignore underlines) is found inside the packet, that means there is an attachment (.scr) in the e-mail (virus). So this packet will suffer the action named 'virus'. This action logs the event, dumps the malicious traffic in tcpdump format and drops the packet. Below is an example of rule against a type of buffer overflow attempt against DNS servers:

<<http://hlbr.sourceforge.net/hlbr-rule-2.gif>>
<http://hlbr.sourceforge.net/hlbr-rule-2.gif>

In this case, due to the use of pipe characters (|), HLBR will check the traffic for the hexadecimal sequence given as an attack signature.

HLBR lets you use rules for blocking attacks against network servers. In order to fully understand it please read documentation at <<http://hlbr.sourceforge.net/ips-en.html>> <http://hlbr.sourceforge.net/ips-en.html>, explanations about the IPS concept including charts.

HLBR homepage is at <<http://hlbr.sourceforge.net>>
<http://hlbr.sourceforge.net>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:eriberto@xxxxxxxxxxxxxxxx>>
Eriberto.

=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.