

[TOOL] Chaosreader – Trace TCP/UDP from Tcpcdump Logs

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0081.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/19/03

To: list@securiteam.com

Date: 19 Oct 2003 17:15:29 +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>

Chaosreader – Trace TCP/UDP from Tcpcdump Logs

DETAILS

<<http://users.tpg.com.au/bdgcvb/>> Chaosreader is "a freeware tool that can trace HTTP sessions from a packet log, displaying which bits are plaintexts. It could be used to help verify that some websites really do utilize encryption. It has been written on Solaris using Perl".

The above description is one use of Chaosreader, it has many features. It takes a snoop (or tcpcdump) log and parses every protocol it can. This includes,

- * Any TCP Session
- * Any UDP Stream
- * HTTP transfers (HTML, JPG, GIF, zip, ...)
- * FTP files (active transfers)
- * telnet sessions (also generates real-time playback scripts)
- * SMTP emails
- * ...

ADDITIONAL INFORMATION

The information has been provided by <<mailto:brendan.gregg@tpg.com.au>>

Securiteam: [TOOL] Chaosreader – Trace TCP/UDP from Tcpdump Logs

Brendan Gregg.

=====

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.