When reporting data out via `mod_log_config` for http.log, I have discovered that \t is reported as \x09. Per apache.org....

---

For security reasons, starting with version 2.0.46, non-printable and other special characters in %r, %i and %o are escaped using \xhh sequences, where hh stands for the hexadecimal representation of the raw byte.... Exceptions from this rule are....all whitespace characters, which are written in their C-style notation ('n, 't, etc).

---

Why are my customformat strings producing x09 in Suricata, when according to `mod_log_config` (which suri points you to) indicates that these should be printed as is, and not hex?

Thanks!

Erik

Related issues:
Related to Feature #602: availability for http.log output - identical to apac...
Ignacio Sanchez wrote:

The special characters are escaped by the libhtp library.

They are actually escaped in Suricata itself. Check util-buffer.[ch].

#6 - 10/13/2012 01:23 PM - Erik C
I looked at util-buffer.h and saw the following, which mimics roughly the same behavior of mod_log_config, but not quite:

(from util-buffer.h)
---
Printable characters are written in the printable format and the non-printable chars are written in hex codes using the |XX| format.
---

If we could just get \t to print as whitespace and not as a hex code, that would make our lives immeasurably wonderful. Thanks for the assist in this! We are looking to move to Suri possibly, and getting this would be the final piece to the puzzle!

#7 - 10/13/2012 03:52 PM - Ignacio Sanchez
I have updated the custom http logging wiki page.

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Custom_http_logging

Please let me know if you find any errors in the documentation, or if you find the logging behaves in a different way.

#8 - 10/15/2012 03:00 AM - Victor Julien
I think we can easily add another print function to create the format of mod_log_config. Ignacio, are you interested in implementing that?

#9 - 10/16/2012 12:56 PM - Ignacio Sanchez

I think we can easily add another print function to create the format of mod_log_config. Ignacio, are you interested in implementing that?

Yes, ok. The feature request is #602

#10 - 10/26/2013 10:23 AM - Victor Julien
- Target version set to TBD

#11 - 12/22/2015 04:14 PM - Andreas Herz
- Status changed from Assigned to Closed

fixed by #602

#12 - 10/19/2017 12:57 AM - Victor Julien
- Target version deleted (TBD)