Suricata - Bug #236

fast log xrefs should be removed.

09/08/2010 02:25 PM - Will Metcalf

| Status: | Closed |
| Priority: | Normal |
| Assignee: | Gurvinder Singh |
| Category: | |
| Target version: | 1.1beta1 |
| Affected Versions: | |
| Difficulty: | |
| Effort: | |
| Label: | |

Description
Currently the suricata fast.log doesn't match the snort fast log. xrefs should be removed from fast log.

Example snort fast logs (ip addy's have been changed)
12/26-11:11:11.012275 [**] [1:2009022:3] ET VIRUS Zlob User Agent - Likely Zlob (securityinternet) [**] [Classification: A Network Trojan was detected] [Priority: 1] [TCP] 10.1.1.1:1033 -> 10.1.1.2:80

History
#1 - 09/08/2010 11:49 PM - Victor Julien
- Subject changed from fast log should fill in protcol name when known by /etc/protocols xrefs should be removed. to fast log xrefs should be removed.

#2 - 09/10/2010 02:44 AM - Victor Julien
- Assignee changed from OISF Dev to Gurvinder Singh
- Estimated time changed from 2.50 h to 5.00 h

#3 - 09/10/2010 02:44 AM - Victor Julien
- Estimated time changed from 5.00 h to 1.00 h

#4 - 09/24/2010 12:33 PM - Gurvinder Singh
- File 0001-removed-xref-from-the-alert-fastlog.patch added
- Status changed from New to Resolved
- % Done changed from 0 to 80

Patch has been attached.

#5 - 09/27/2010 02:46 AM - Victor Julien
- Status changed from Resolved to Closed
- % Done changed from 80 to 100

Patch applied to my local tree, thanks Gurvinder.

Files
0001-removed-xref-from-the-alert-fastlog.patch 3.29 KB 09/24/2010 Gurvinder Singh