Suricata - Bug #188
Snort now supports byte_test <= >= operators so should we.
06/25/2010 07:44 AM - Will Metcalf

Status: Closed
Priority: Normal
Assignee: Gurvinder Singh
Category: 
Target version: 1.1beta1
Affected Versions: 
Effort: 
Description
It seems somewhere along the way snort implemented support for <= >= for byte_test and currently VRT rule sid:16603 uses a byte_test operator in this way. We should support the same. The example rules below should all match when processing the attached pcap.

```
alert tcp any any -> any any (msg:"content + byte_test + relative"; content:"GET "; depth:4; content:"HTTP/1."); byte_test:1,=,0,0,relative,string,dec; classtype:bad-unknown; sid:123; rev:1);
alert tcp any any -> any any (msg:"content + byte_test + relative"; content:"GET "; depth:4; content:"HTTP/1."); byte_test:1,<=,0,0,relative,string,dec; classtype:bad-unknown; sid:124; rev:1);
alert tcp any any -> any any (msg:"content + byte_test + relative"; content:"GET "; depth:4; content:"HTTP/1."); byte_test:1,>=,0,0,relative,string,dec; classtype:bad-unknown; sid:125; rev:1);
```

History

#1 - 11/15/2010 12:31 AM - Victor Julien
- Due date set to 11/19/2010
- Status changed from New to Assigned
- Assignee changed from Victor Julien to Gurvinder Singh
- Target version changed from TBD to 1.1beta1

Gurvinder, adding this shouldn't be hard. Can you do this and unittest it as well?

#2 - 11/15/2010 06:28 PM - Gurvinder Singh
- File 0001-add-the-support-for-and-operator-for-byte_test.patch added
- Status changed from Assigned to Resolved
- % Done changed from 0 to 90

Attached patch added the support for above mentioned operators.

#3 - 11/17/2010 02:50 AM - Victor Julien
- Status changed from Resolved to Closed
- % Done changed from 90 to 100

Patch applied, thanks Gurvinder.

Files

```
allworkandnoplayplain.pcap  2.7 KB  06/25/2010  Will Metcalf
0001-add-the-support-for-and-operator-for-byte_test.patch  5.11 KB  11/15/2010  Gurvinder Singh
```