Suricata - Bug #2798
--engine-analysis is unaware of http_host buffer
02/01/2019 05:50 PM - Travis Green

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Travis Green</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0beta1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

### Description

Using --engine-analysis flag produces incorrect output for engine analysis:

```
-- Sid: 1111111 =
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TESTRULE Bug: Engine analysis warnings for http_host"; flow:established,to_server; content:"funkyhost.org"; http_host; pcre:"/funk/W"; sid:111111;)
    App layer protocol is http.
    Rule contains 0 content options, 0 http content options, 1 pcre options, and 0 pcre options with http modifiers.
    Fast Pattern "funkyhost.org" on "http host header (http_host)" buffer.
    Warning: Rule uses pcre without a content option present.
    -Consider adding a content to improve performance of this rule.
    Warning: Rule app layer protocol is http, but pcre options do not have http modifiers.
    -Consider adding http pcre modifiers.
```

consider updating detect-engine-analyzer.c to reflect

### History

#### #1 - 02/01/2019 08:21 PM - Travis Green
Submitted PR.

#### #2 - 02/21/2019 10:31 AM - Victor Julien
- Status changed from New to Closed
- Target version set to 5.0beta1

[https://github.com/OISF/suricata/pull/3660](https://github.com/OISF/suricata/pull/3660)