Suricata - Feature #273
IRC protocol detection support
02/28/2011 04:56 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
<tr>
<td>Label:</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

**Description**
Support IRC in the protocol detection module so we can write rules like:
alert irc ....

**Related issues:**
- Related to Feature #2757: improve protocol detection
- Related to Bug #2978: IRC traffic parsed by FTP
- Related to Task #4151: Research: New protocol support
- Related to Task #4097: Suricon 2020 brainstorm
- Blocked by Feature #2572: extend protocol detection to specify flow direction

**History**

#1 - 04/11/2011 01:31 AM - Victor Julien
- Target version changed from 1.1beta2 to 1.1beta3

#2 - 04/21/2011 03:32 AM - Victor Julien
- Due date set to 04/29/2011
- Assignee changed from Victor Julien to Anoop Saldanha
- Estimated time set to 6.00 h

Anoop can you create a "probing parser" on top of task 209? Thanks!

#3 - 04/21/2011 04:02 AM - Anoop Saldanha
Victor Julien wrote:

Anoop can you create a "probing parser" on top of task 209? Thanks!

cool

#4 - 10/19/2011 05:06 AM - Victor Julien
- Target version changed from 1.1beta3 to 1.2

Retargeting to version 1.2 as some interaction issues with the ftp parser need to be addressed first.

#5 - 01/10/2012 10:31 AM - Victor Julien
- Target version changed from 1.2 to TBD

#6 - 09/08/2016 03:32 PM - Andreas Herz
- Assignee changed from Anoop Saldanha to OISF Dev

Is this still a thing to have dedicated IRC rules? :)

#7 - 05/30/2018 08:04 AM - Victor Julien
This depends on protocol detection improvements. Right now patterns for ftp, smtp, and irc would be too similar and the proto detection is too dumb.

#8 - 08/09/2018 07:47 AM - Victor Julien
- Blocked by Feature #2572: extend protocol detection to specify flow direction added

#9 - 12/21/2018 12:07 PM - Victor Julien
- Related to Feature #2757: improve protocol detection added

#10 - 03/11/2019 02:06 PM - Victor Julien
- Assignee set to Community Ticket

#11 - 05/10/2019 07:59 AM - Victor Julien
- Related to Bug #2978: IRC traffic parsed by FTP added

#12 - 11/19/2020 09:22 PM - Victor Julien
- Related to Task #4151: Research: New protocol support added

#13 - 11/23/2020 01:45 PM - Victor Julien
- Related to Task #4097: Suricon 2020 brainstorm added

#14 - 12/24/2020 07:06 AM - Victor Julien
- Label Protocol added