Suricata - Feature #2519
XFF iprep support
06/18/2018 05:15 PM - chris lujan

<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>high</td>
</tr>
</tbody>
</table>

Description
I have made many attempts and I am fairly confident that when xff is enabled (in overwrite mode), iprep is not applied to the overwritten field and does not alert.

My method of testing was:
1) GET / request to the webserver behind the load-balancer from a tor-browser (using an IP in iprep list), no alerts.
2) GET /uid=0(root) gid=0(root) groups=0(root) request to the webserver behind the load-balancer from a tor-browser (using an IP in iprep list), GPL ATTACK_RESPONSE id check returned root alert present, XFF ip present in src_ip field (src_ip found in iprep files).
3) Make GET request to IP found in iprep list (ET TOR Known Tor Exit Node Traffic group 7 && OTX internal host talking to host known in pulse alerted).
4) Change iprep rule from $HOME_NET any -> any any to any any -> any any, retry steps 1-3, same results.

History
#1 - 06/19/2018 08:28 PM - Andreas Herz
  - Assignee set to Anonymous
  - Target version set to TBD

could you prepare a pcap?

#2 - 06/23/2018 10:05 AM - Victor Julien
  - Tracker changed from Bug to Feature
  - Effort set to medium
  - Difficulty set to high
  - Affected Versions deleted (4.0.4)

XFF is currently only used for output. Detection support would mean the detection engine would need to become aware of XFF.

#3 - 02/23/2019 10:03 PM - Andreas Herz
  - Assignee set to Community Ticket