Suricata - Feature #4398

support regex match and flowvars as keywords value

03/15/2021 10:27 AM - jim cookie

<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></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>
</tbody>
</table>

**Description**

if we want to detect java jndi injection such as fastjson rce:
tcp payload content:
ldap://192.168.204.1:888 or rmi://192.168.204.1:888
flow rules just only detect the first steps of jndi injection:
alert tcp any any -> any any
   (msg:"TCP_LDAP_Injection";pcre:/(ldap://(\S{2,256}):([0-9]{2,5})\//),flow:ldap,flow:ldap_url,flow:ldap_port;sid:10001;rev:1;)
we can found flowvars ldap, ldap_url and ldap_port in eve.json:

```
{
    "timestamp": "2021-01-12T14:10:04.520436+0800",
    "flow_id": 60042522718452,
    "pcap_cnt": 3,
    "event_type": "alert",
    "src_ip": "192.168.204.130",
    "src_port": 20,
    "dest_ip": "192.168.204.128",
    "dest_port": 80,
    "proto": "TCP",
    "metadata": {
        "flowvars": [{
            "ldap": "ldap://192.168.204.1:888/",
            "ldap_url": "192.168.204.1",
            "ldap_port": 888
        }],
        "alert": {
            "action": "allowed",
            "gid": 1,
            "signature_id": 10001,
            "rev": 1,
            "signature": "TCP_LDAP_Injection",
            "category": "",
            "severity": 3,
            "flow": {
                "pkts_toserver": 0,
                "bytes_toserver": 84,
                "bytes_toclient": 0,
                "start": "2021-01-12T14:10:04.520436+0800",
                "payload": "R0VUIC9sZGFwOi8vMTkyLjE2OC4yMDQuMTo4ODgv",
                "payload_printable": "GET /ldap://192.168.204.1:888/",
                "stream": 0
            }
        }
    }
}
```
but we can't detect the hackers ldap server : 192.168.204.1 connection .
if we suricata support use regex match and flowvars as keywords value .we can creat rules like this:
alert tcp any any -> any any
   (msg:"TCP_LDAP_Injection_steps1";pcre:/(ldap://(\S{2,256}):([0-9]{2,5})\//),flow:ldap,flow:ldap_url,flow:ldap_port;noalert;sid:10001;rev:1;)
alert tcp any any -> $ldap_url $ldap_port (msg:"TCP_LDAP_Injection_success";sid:10002;rev:1;)
maby also with xbnts work great more.

-----------------------------------------------------------------------------------
have any other ways to detect jndi injection ?
thanks you !