Suricata - Feature #5152

Anomaly: CredSSP support addition to Suricata anomaly parsing

02/23/2022 10:40 AM - Peter Manev

<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>OISF Dev</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

CredSSP can be used for http authentication, it may not be the best option in terms of security but it is available. [https://docs.microsoft.com/en-us/powershell/module/microsoft.wsman.management/enable-wsmancredssp?view=powershell-7.2](https://docs.microsoft.com/en-us/powershell/module/microsoft.wsman.management/enable-wsmancredssp?view=powershell-7.2)

Currently suricata generates an anomaly event (REQUEST_AUTH_UNRECOGNIZED) on inspecting http auth with CredSSP that could result in millions such events in a organisational setup with lots of powershell usage for example.

```
{
  "timestamp": "2021-11-15T17:29:46.150405+0100",
  "flow_id": 1858400320896909,
  "pcap_cnt": 131,
  "event_type": "anomaly",
  "src_ip": "ip.ip.ip.ip",
  "src_port": 5985,
  "dest_ip": "ip.ip.ip.ip",
  "dest_port": 64848,
  "proto": "TCP",
  "tx_id": 0,
  "anomaly": {
    "app_proto": "http",
    "type": "applayer",
    "event": "REQUEST_AUTH_UNRECOGNIZED",
    "layer": "proto_parser"
  }
},
{
  "timestamp": "2021-11-15T17:29:46.152065+0100",
  "flow_id": 1858400320896909,
  "pcap_cnt": 132,
  "event_type": "http",
  "src_ip": "ip.ip.ip.ip",
  "src_port": 64848,
  "dest_ip": "ip.ip.ip.ip",
  "dest_port": 5985,
  "proto": "TCP",
  "tx_id": 0,
  "http": {
    "hostname": "hostrandom",
    "http_port": 5985,
    "url": "/wsman/?PSVersion=5.1.15743.2084",
    "http_user_agent": "Microsoft WinRM Client",
    "http_method": "POST",
    "protocol": "HTTP/1.1",
    "status": 401,
    "length": 0,
    "request_headers": [
      {
        "name": "Connection",
        "value": "Keep-Alive"
      }
    ]
  }
}
```
I have a private TLPRED pcap data I can test with if needed.