I'm not sure this is really a bug or maybe just some confusion due to the lack of documentation, or if dcerpc probing is not working in this use case.

Consider the 3 rules, I would expect all three of them to fire given the use case of DCERPC nested in SMB (though I could understand if only sid:1 fires)

```
alert dcerpc any any -> any any (msg:"ET POLICY DCERPC SVCCTL OpenSCManagerW Request"; flow:established,to_server; dcerpc.iface:367abb81-9844-35f1-ad32-98f038001003; dcerpc.opnum:15; classtype:bad-unknown; sid:1; rev:1;)
alert smb any any -> any any (msg:"ET POLICY DCERPC SVCCTL OpenSCManagerW Request"; flow:established,to_server; dcerpc.iface:367abb81-9844-35f1-ad32-98f038001003; dcerpc.opnum:15; classtype:bad-unknown; sid:2; rev:1;)
alert tcp any any -> any [135,139,445,1024:] (msg:"ET POLICY DCERPC SVCCTL OpenSCManagerW Request"; flow:established,to_server; dcerpc.iface:367abb81-9844-35f1-ad32-98f038001003; dcerpc.opnum:15; classtype:bad-unknown; sid:3; rev:1;)
```

sid:3 is taken directly from suricata-test


However, When running these rules against the attached pcap, only sid:2 and sid:3 fire with gitmaster, which is unexpected to me. It would appear that the DCERPC protocol is not matching when it's nested in SMB, though the dcerpc keywords work fine when using the SMB protocol, so not sure what's going on there.

<table>
<thead>
<tr>
<th>Subtasks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bug # 5395: DCERPC protocol detection when nested in SMB (6.0.x backport)</td>
</tr>
<tr>
<td>Bug # 5423: DCERPC protocol detection when nested in SMB (5.0.x backport)</td>
</tr>
</tbody>
</table>

History:

#1 - 03/25/2022 04:31 PM - Peter Manev
Yes I can confirm the same ,was testing it a few weeks back, forgot to put in an issue.
Related to https://redmine.openinfosecfoundation.org/issues/5134 in terms of perf.

#2 - 03/28/2022 02:43 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Victor Julien
- Target version changed from TBD to 7.0rc1

#3 - 03/28/2022 04:27 PM - Shivani Bhardwaj
s-v test (needs updation): https://github.com/OISF/suricata-verify/pull/798

#4 - 06/09/2022 11:31 AM - Victor Julien
Some observations:

The alert dcerpc doesn't match because the app layer protocol of the traffic isn't dcerpc, its smb. However alert dcerpc locks the rule to the "pure" dcerpc.
However if we don't specify the protocol, so use alert ip or alert tcp, it will do what you expect:

```json

"raw": "alert ip any any -> any any (msg:"ET POLICY DCERPC SVCCTL OpenSCManagerW Request"; flow:established,to_server; dcerpc.iface:367abb81-9844-35f1-ad32-98f038001003; dcerpc.opnum:15; classtype:bad-unknown; sid:4; rev:1))",
"id": 4,
"gid": 1,
"rev": 1,
"msg": "ET POLICY DCERPC SVCCTL OpenSCManagerW Request",
"requirements": [
  "flow",
  "dcerpc"
],
"flags": [
  "src_any",
  "dst_any",
  "applayer",
  "toserver"
],
"pkt_engines": [
  {
    "name": "packet",
    "is_mpm": false
  }
],
"frame_engines": [],
"engines": [
  {
    "name": "dce_generic",
    "direction": "toserver",
    "is_mpm": false,
    "app_proto": "dcerpc",
    "progress": 0,
    "matches": [
      {
        "name": "dcerpc.iface"
      },
      {
        "name": "dcerpc.opnum"
      }
    ]
  }
],
"lists": {
  "packet": {
    "matches": [
      {
        "name": "flow"
      }
    ]
  }
}
```
This is because the keywords internally can handle both "pure" dcerpc and smb with dcerpc running over it, so the rule is setup to handle both.

So I guess the question is if the dcerpc app protocol specification in the rule should be overloaded to mean "either exact dcerpc or dcerpc over smb".

#5 - 06/10/2022 10:44 AM - Victor Julien
- Status changed from Assigned to In Review
- Label Needs backport to 5.0, Needs backport to 6.0 added

https://github.com/OISF/suricata/pull/7522

#6 - 06/10/2022 08:51 PM - Brandon Murphy

So I guess the question is if the dcerpc app protocol specification in the rule should be overloaded to mean "either exact dcerpc or dcerpc over smb".
I'm personally in favor of the rule being "overloaded". It makes sense from a rule writers perspective.

#7 - 06/14/2022 05:53 AM - Victor Julien
- Status changed from In Review to Resolved

https://github.com/OISF/suricata/pull/7534/commits/a83f02d4cda9e98111162907b20c078c8603a085

#8 - 07/01/2022 09:50 AM - Victor Julien
- Label deleted (Needs backport to 6.0)

#9 - 07/01/2022 10:40 AM - Victor Julien
- Status changed from Resolved to Closed

#10 - 07/01/2022 10:54 AM - Victor Julien
- Label deleted (Needs backport to 5.0)

**Files**

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>cool_1.pcap</td>
<td>377 KB</td>
<td>03/25/2022</td>
<td>Brandon Murphy</td>
</tr>
</tbody>
</table>