



Suricata IPS Log Analysis Questions

By: Ryan Stewart

1. What SSL vulnerability is targeted in the Suricata IPS log?

```
suricata.log [x] new 1 [x]
{"timestamp":"2017-03-24T14:00:03.928247-0600","flow_id":"1603540984452599","pcap_cnt":470307,"event_type":
_ip":"10.60.11.10","src_port":443,"dest_ip":"10.60.11.20","dest_port":40170,"proto":"TCP","tx_id":0,"aler
:"allowed","gid":1,"signature_id":2019415,"rev":3,"signature":"ET POLICY SSLv3 inbound connection to serv
vulnerable to POODLE attack","category":"Potential Corporate Privacy
Violation","severity":1,"tls":{"version":"SSLv3"},"app_proto":"tls","flow":{"pkts_toserver":10,"pkts_toc
tes_toserver":1650,"bytes_toclient":866,"start":"2017-03-24T14:00:02.775671-0600"}}}
```

2. Which scanning tool triggers the Suricata IPS log?

```
": "2017-03-24T14:00:04.963563-0600","flow_id":"275867809011165","pcap_cnt":482098,"event_type":"alert","src_
.113.45","src_port":57428,"dest_ip":"192.168.113.55","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"acti
","gid":1,"signature_id":2024364,"rev":3,"signature":"ET SCAN Possible Nmap User-Agent
category":"Web Application
verity":1,"http":{"hostname":"192.168.113.78","url":"/","http_user_agent":"Mozilla/5.0 (compatible; Nmap
ngine;
p.org/book/nse.html)","http_method":"GET","protocol":"HTTP/1.1","status":401,"length":18},"app_proto":"htt
pkts_toserver":7,"pkts_toclient":4,"bytes_toserver":862,"bytes_toclient":612,"start":"2017-03-24T14:00:02.
}}}
```

3. Does the Suricata IPS log indicate a successful execution of the command?

```
suricata.log [x]
": "2017-03-24T18:05:58.530985-0600","flow_id":"1682285881575487","pcap_cnt":483653,"event_type":"alert","src
8.59.71","src_port":80,"dest_ip":"192.168.59.81","dest_port":56040,"proto":"TCP","alert":{"action":"allowe
signature_id":2017025,"rev":3,"signature":"ET ATTACK_RESPONSE Net User Command
category":"Successful User Privilege
rity":1,"flow":{"pkts_toserver":12,"pkts_toclient":7,"bytes_toserver":4776,"bytes_toclient":4428,"start":
18:05:53.575551-0600}}}
```

