Net Flow Analysis Questions

By: Ryan Stewart

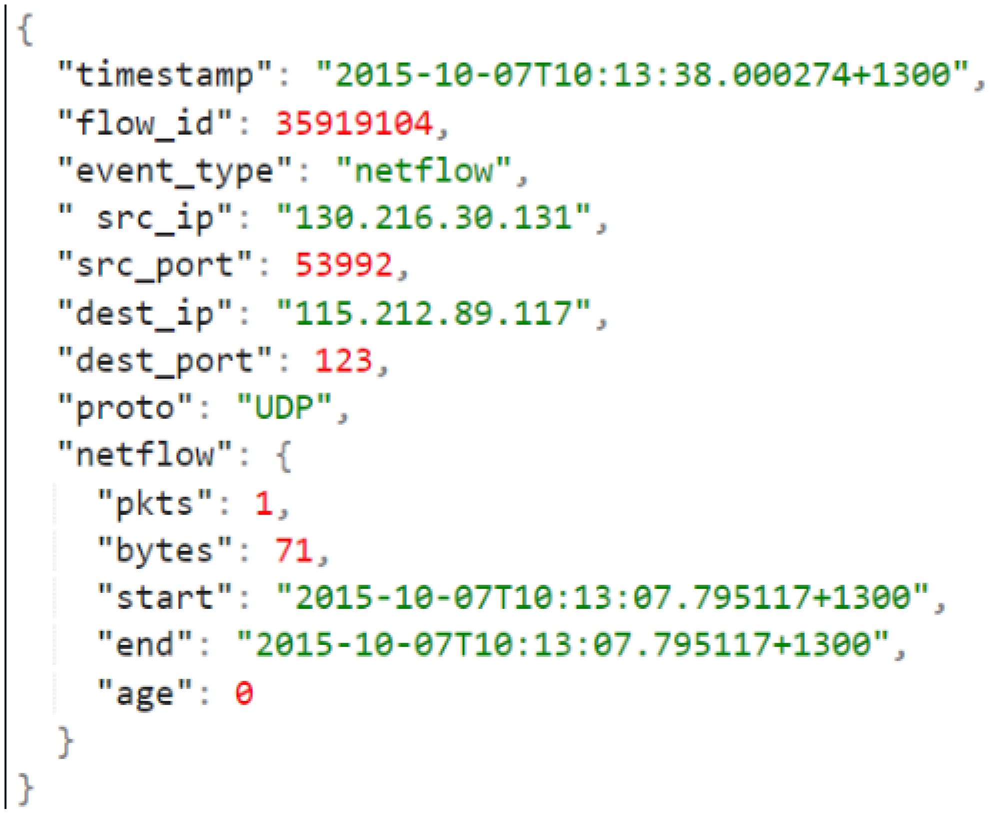
Types of Attacks Detectable with Netflow Data

Question: What types of attacks can be detected with Netflow data?

- Network Anomaly Detection
- Detection of an Infected System
- Detection of malicious applications running on the Endpoint
- Suspicious Domain Requests

Which of the following are not produced through Netflow logs?

- IP Information
- XFF IP Information
- Port Information
- Interface Information



```
{
  "timestamp": "2015-10-07T10:13:38.000274+1300",
  "flow_id": 35919104,
  "event_type": "netflow",
  " src_ip": "130.216.30.131",
  "src_port": 53992,
  "dest_ip": "115.212.89.117",
  "dest_port": 123,
  "proto": "UDP",
  "netflow": {
    "pkts": 1,
    "bytes": 71,
    "start": "2015-10-07T10:13:07.795117+1300",
    "end": "2015-10-07T10:13:07.795117+1300",
    "age": 0
  }
}
```

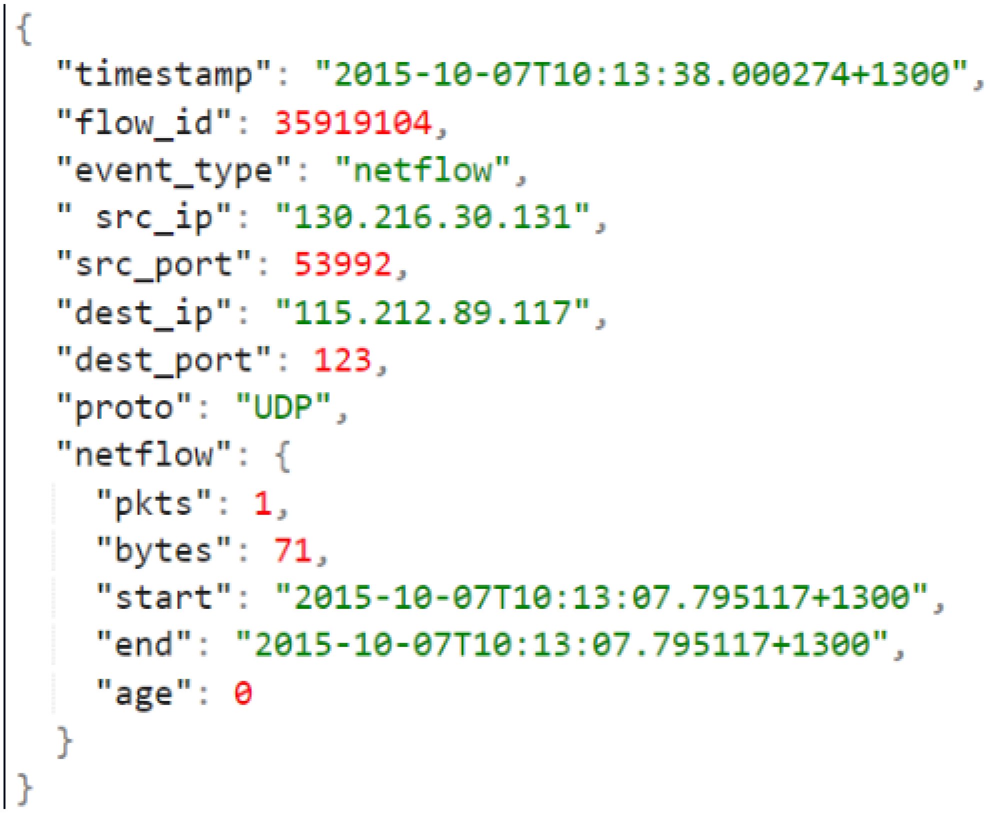
NetFlow Data Examination

Question: Which of the following is not true according to the NetFlow data above?

A) Total number of packages is 1.

B) The amount of data transmitted is 71 bytes.

C) NTP service is definitely running on the target port 123.



```
{
  "timestamp": "2015-10-07T10:13:38.000274+1300",
  "flow_id": 35919104,
  "event_type": "netflow",
  " src_ip": "130.216.30.131",
  "src_port": 53992,
  "dest_ip": "115.212.89.117",
  "dest_port": 123,
  "proto": "UDP",
  "netflow": {
    "pkts": 1,
    "bytes": 71,
    "start": "2015-10-07T10:13:07.795117+1300",
    "end": "2015-10-07T10:13:07.795117+1300",
    "age": 0
  }
}
```

NetFlow Anomaly Identification

Question: According to the NetFlow data above, what could it be to see 10k requests from different source IPs to the same destination within 2 minutes?

- SYN Flood
- UDP Flood
- ICMP Flood
- DNS Flood

Application Layer Information with Netflow

Question: Can "Layer 7 - Application Layer" information be obtained with Netflow analysis?

Answer: No