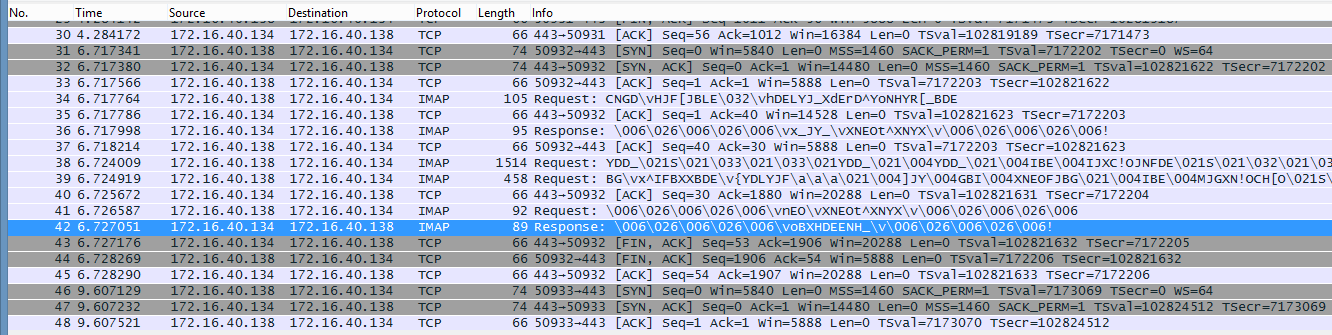
Solution:

All the TCP handshake requests are initiated by 172.163.40.138. It chooses a random port and increments for subsequent requests. The request is always made to 172.16.40.134 on port 443.

After analyzing the file using wire shark; tried to decode the TCP to other formats like IMAP, SSH, DNS etc. I saw some changes; however I could not retrieve any message from it. IMAP made most sense when the SSH Continuous data got transformed to Requests and responses



To begin with snort rules I would expect the header part to e as below:

**Alert tcp 172.163.40.138 any -> 172.16.40.134 443 (msg:”ALERT! Assignment 5 - Connection Initiation! “; flags: s; sid:1000001);**

**alert tcp 172.16.40.138 any -> 172.16.40.134 443 (msg:”ALERT! Fishy request packet “; sid:1000005; content:"|43 4E 47 44|"; rawbytes;)**

I noticed that all the initial request packets have a common repeating text “CNGD” hence we search the hex equivalent 43 4E 47 44 in raw bytes.

The above rule gives an alert when the first request packet is sent.

Below is the screenshot after running the pcap against the rules

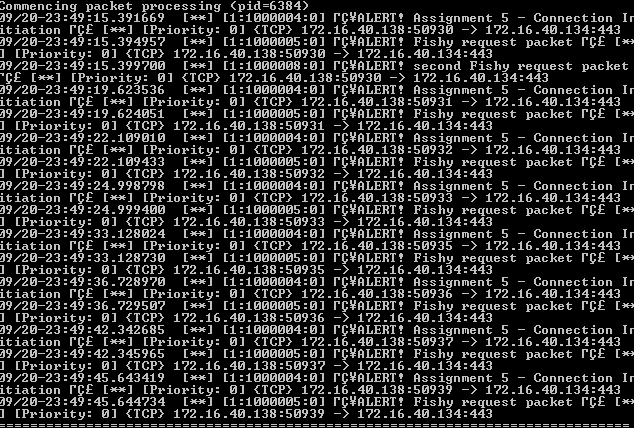


-i is to select the interface

-c is to choose the conf file

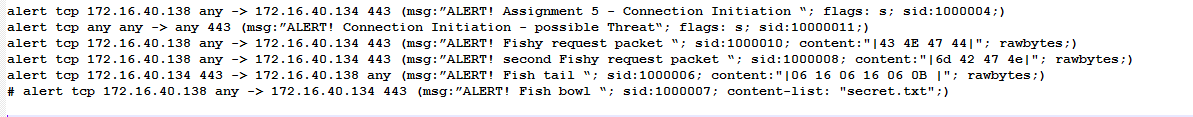
-A is to display the output on the console

-r is to provide the pcap file as input

Below is the output received

I am able to capture alerts for connection initiation and first request packet.

I wrote some more rules, however I could not capture any response packets. Below are my rules



Fields:

|  |  |  |
| --- | --- | --- |
| Action: | **Alert** | because we need an alert to pop up when a snort rule matches |
| Protocol: | **tcp** | because the protocol under analysis from the given pcap is TCP |
| SRC IP adderess : | **172.163.40.138** | because the TCP handshake is being initiated by 172.163.40.138 |
| SRC port : | **any** | because in the pcap 172.163.40.138 chooses a random port and increases the port number for subsequent requests |
| Direction operator: | **->** | direction of traffic for this rule |
| Dest IP : | **172.16.40.134** | TCP request is made to 172.16.40.134 from the source |
| Dest port: | **443** | port for 172.16.40.134 |
| Msg: | **ALERT! Assignment 5 - Connection Initiation** | Message to be displayed |
| Flags : | **S** | because we want to check for the case when the flag is set to SYN |
| Sid : | **1000001** | Assign a Snort id to the rule |

This above rule would give an alert when 172.163.40.138 tries to initiate a connection to 172.16.40.134 on port 443.

**alert tcp 172.16.40.138 any -> 172.16.40.134 443 (msg:”ALERT! Fishy request packet “; sid:1000005; content:"|43 4E 47 44|"; rawbytes;)**

I noticed that all the initial request packets have a common repeating text “CNGD” hence we search the hex equivalent 43 4E 47 44 in raw bytes.

The above rule gives an alert when the first request packet is sent.