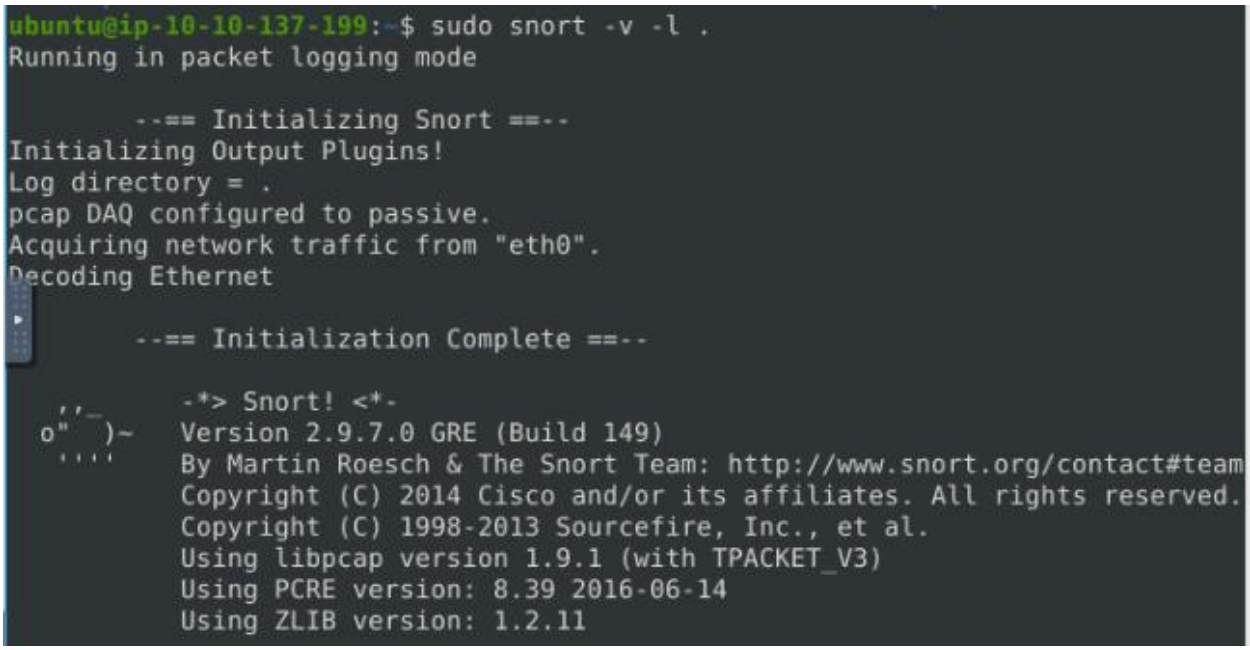
Snort Challenge - Live Attacks

Task:

I am tasked with protecting a coffee retail company's digital assets, particularly a secret recipe, from cyberattacks. J.A.V.A., an AI assistant, is alerting me to a brute-force attack on the company's system. The AI advises I use Snort, an intrusion detection system, to monitor network traffic, identify the anomaly, and create a rule to mitigate the attack. The task at hand is to analyze the network for signs of intrusion and implement a security rule to stop the brute-force attack.

Steps:

1. **Run Snort in Sniffer Mode**: Use the command `sudo snort -v -l .` to start Snort in sniffer mode and log data in the current directory. Let it run for 10-15 seconds, then stop it by pressing `ctrl + c`.



2. **Inspect the Log File**: Use the command `sudo snort -r snort.log.1672697486 -X` to view the captured packets in the log file.

```
ubuntu@ip-10-10-137-199:~$ sudo snort -r snort.log.1672697486 -X
```

3. **Search for Suspicious Port 4444**: Run `sudo snort -r snort.log.1672697486 -X | grep ":4444"` to search for packets using port 4444, which might indicate a reverse shell.

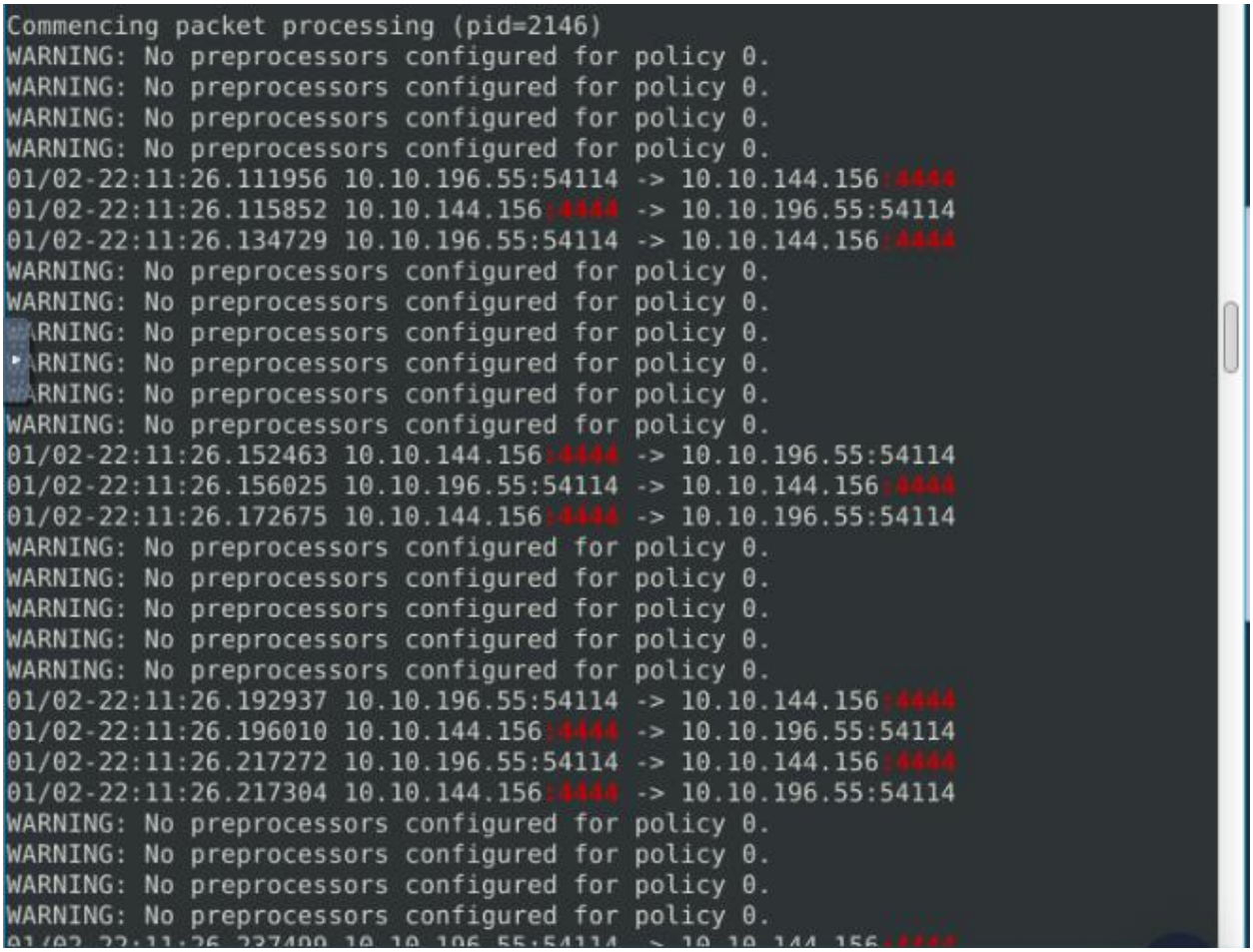
```
ubuntu@ip-10-10-137-199:~$ sudo snort -r snort.log.1672697486 -X | grep ":4444"
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to read-file.
Acquiring network traffic from "snort.log.1672697486".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

The results indicate help show I’m in the right direction with the investigation.



4. **Limit the Results**: Use `sudo snort -r snort.log.1672697486 -X -n 10` to view only the first 10 results from the log file.
5. **Open Local Rules File**: Open the local.rules file by running `sudo gedit /etc/snort/rules/local.rules` in a text editor.
6. **Write the Drop Rule**: Write a Snort rule with `drop tcp any 4444 <> any any (msg:"Reverse Shell Detected"; sid:100001; rev:1;)` to block traffic on port 4444.

```
7
8 drop tcp any 4444 <> any any (msg:"Reverse Shell Detected"; sid:100001; rev:1;)
```

7. **Save the Rule**: Save the rule by pressing `ctrl + s` and exit the text editor.
8. **Run Snort with the New Rule**: Run Snort using the command `sudo snort -c /etc/snort/snort.conf -q -Q --daq afpacket -i eth0:eth1 -A full` to apply the rule to live traffic.

9. **Stop Snort and Get the Flag**: Once the malicious traffic was stopped for about a minute, a `flag.txt` file appeared on the desktop. Stop Snort with `ctrl + c`. Double-click the flag.txt file to open it.

Conclusion:

In this task, I used Snort to monitor network traffic and identify suspicious activity related to port 4444, which indicated a potential reverse shell attack. After inspecting the log file, I created a custom "drop" rule to block TCP traffic on port 4444, ensuring a proactive defense against future threats. I applied the rule to live traffic, and once Snort detected and stopped the attack, a flag file appeared, confirming the success of my efforts.