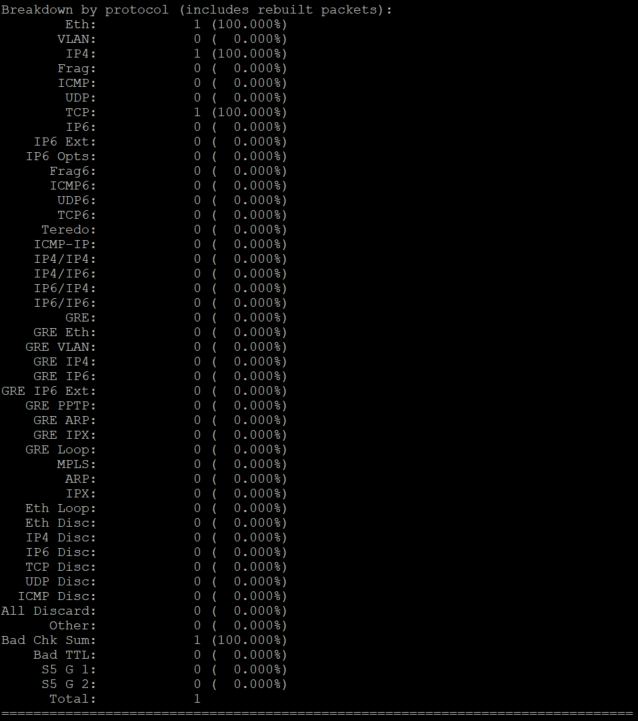
## **Task 1**: Discovery Flag: Display data-link headers and the application layer data

* **Solution:**

|  |
| --- |
| Sudo snort -de |

* + d: show application data in transit
  + Text

    Description automatically generatede: show the data link layer headers

**research:** http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node4.html

## **Task 2**: Capture only ICMP

* **Solution:**

|  |
| --- |
| Sudo snort -vde icmp |

* + Snort use sniffer mode and apply BPF filter that only retrieve ICMP packet.

Text

Description automatically generated

## **Task 3:** Check Alerts

**Created Rule:**

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Since this rule will generate an alert message for every single captured IP packet that will used up the disk space. And its hard to find the right message as its loaded with alerts if it keeps capture packets

## **Task 4:** Alert for Only ICMP

Text, application

Description automatically generated

Text

Description automatically generated

## **Task 5:** Snort Rule

Company name

Description automatically generated with low confidence

The subnet 192.168.1.0/24 can send TCP traffic to 192.168.1.0/24 and the port number less and equal than 1024 will not create any alert. Else does.

**TASK 6:** Alert on HTTP Get

Since HTTP clients generally use TCP connections to communicate to the Server, so that we will monitor the TCP traffic. (As my Raspberry pi cannot use browser, so I changed to Kali)

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

Normally server usually host http request at port 80. So we monitor the destination address with Port 80.

**TASK 7:** Alert on TCP Flags

Text

Description automatically generated

Text

Description automatically generated A screenshot of a computer

Description automatically generated with medium confidence

**Task 8:** Alert on Telnet

A screenshot of a computer

Description automatically generated with medium confidence

A picture containing text

Description automatically generated