Task 4

4.1

(Content with pipes means it’s a binary value )

PNG- 89504E470D0A1A0A

Snort rule - alert tcp any any <> any any (msg:"PNG File Detected"; content:"|89504E470D0A1A0A|"; sid:100008; rev:1;)

Execute - sudo snort -c local.rules -r ftp-png-gif.pcap -l .

Analyze snort log - sudo snort -d -r snort.log.1687029270

(log file name will vary depending on your file name)

-d for display full packet details

-r for reading the snort log packet

A screenshot of a computer

Description automatically generated

4.2

alert tcp any any <> any any (msg:"PNG File Detected"; content:"GIF89a"; sid:100008; rev:1;)

alert tcp any any <> any any (msg:"PNG File Detected"; content:"GIF87a"; sid:100009; rev:2;)

A screenshot of a computer

Description automatically generated

--­--------­--------­--------­--------­--------­--------­--------­--------­--------­--------­--------­--------­--------­--------­--------­-----