Task 6

6.1

alert tcp any 3372 -> any any (msg: "Troubleshooting 1"; sid:1000001; rev:1;)

add an extra space after destination port number.

A screenshot of a computer screen

Description automatically generated with medium confidence

6.2

alert icmp any any -> any any (msg: "Troubleshooting 2"; sid:1000001; rev:1;)

(add source port number)

A screenshot of a computer screen

Description automatically generated with medium confidence

6.3

alert icmp any any -> any any (msg: "ICMP Packet Found"; sid:1000001; rev:1;)

alert tcp any any -> any 80,443 (msg: "HTTPX Packet Found"; sid:1000002; rev:2;)

(different rules should have different sid and rev )

A screenshot of a computer screen

Description automatically generated with medium confidence

6.4

alert icmp any any -> any any (msg: "ICMP Packet Found"; sid:1000001; rev:1;)

alert tcp any 80,443 -> any any (msg: "HTTPX Packet Found"; sid:1000002; rev:2;)

A screenshot of a computer screen

Description automatically generated with medium confidence

6.5

alert icmp any any <> any any (msg: "ICMP Packet Found"; sid:1000001; rev:1;)

alert icmp any any <> any any (msg: "Inbound ICMP Packet Found"; sid:1000002; rev:1;)

alert tcp any any -> any 80,443 (msg: "HTTPX Packet Found"; sid:1000003; rev:1;)

(<- no direction with this symbol for rule 2 and change : with ; in rules 3)

A screenshot of a computer screen

Description automatically generated with medium confidence

6.6

alert tcp any any <> any 80 (msg: "GET Request Found"; content:"GET"; sid: 100001; rev:1;)A screenshot of a computer screen

Description automatically generated with medium confidence

6.7

Msg

Screens screenshot of a computer screen

Description automatically generated with low confidence

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