**Part 3: Custom rules & Explanation.**

**Rule 1:**

**alert tcp any any -> 192.168.1.1 54321 (msg:"Student packet detected"; content:"Christos-2021030183"; sid:1000001; rev:1;)**

Detects TCP packets targeting IP**192.168.1.1** on port **54321** containing content

“Christos-2021030183”.

Alert: "Student packet detected"

**Rule 2:**

**alert tcp any any -> 192.168.1.2 80 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000002; rev:1;)**

Detects TCP packets targeting IP1**92.168.1.2** on port **80** containing content “Christos-2021030183”.

Alert: "Port scan packet detected"

**Rule 3:**

**alert tcp any any -> 192.168.1.2 443 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000003; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **443** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 4:**

**alert tcp any any -> 192.168.1.2 22 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000004; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **22** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 5:**

**alert tcp any any -> 192.168.1.2 23 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000005; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **23** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 6:**

**alert tcp any any -> 192.168.1.2 21 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000006; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **21** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 7:**

**alert udp any any -> 192.168.1.2 53 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000007; rev:1;)**

Detects UDP packets targeting IP **192.168.1.2** on port **53** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 8:**

**alert tcp any any -> 192.168.1.2 554 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000008; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **554** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 9:**

**alert tcp any any -> 192.168.1.2 3306 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000009; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **3306** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 10:**

**alert tcp any any -> 192.168.1.2 3389 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000010; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **3389** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 11:**

**alert tcp any any -> 192.168.1.2 1883 (msg:"Port scan packet detected"; content:"Christos-2021030183"; sid:1000011; rev:1;)**

Detects TCP packets targeting IP **192.168.1.2** on port **1883** containing content “Christos-2021030183”.

**Alert**: "Port scan packet detected"

**Rule 12:**

**alert tcp any any -> 192.168.1.3 8080 (msg:"Malicious packet detected"; content:"MjAyMTAzMDE4Mw=="; sid:1000012; rev:1;)**

Detects TCP packets targeting IP 192.168.1.3 on port 8080 containing content “MjAyMTAzMDE4Mw==”.

**Alert**: "Malicious packet detected"

**Rule 13-16:**

Identical to Rule 12. Same alert and detection criteria.

**Rule 17:**

**alert udp any any -> 127.0.0.53 53 (msg:"Suspicious domain packet detected"; content:"malicious.example.com"; sid:1000017; rev:1;)**

Detects UDP packets targeting IP **127.0.0.53** on port **53** containing domain “malicious.example.com”.

**Alert**: "Suspicious domain packet detected"

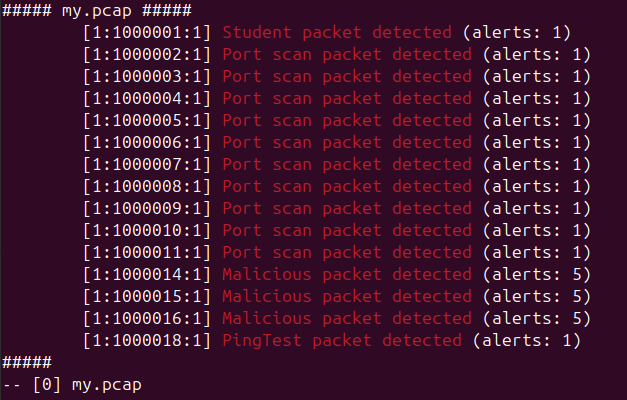
**Rule 18:**

**alert icmp any any -> 192.168.1.4 (msg:"PingTest packet detected"; content:"PingTest-2024"; sid:1000018; rev:1;)**

Detects ICMP packets targeting IP **192.168.1.4** with content “PingTest-2024”.

**Alert**: "PingTest packet detected"

**Screenshot of alerts**

****